UNETHICAL BEHAVIOR USING INFORMATION TECHNOLOGY

.

By

SUTIRTHA CHATTERJEE

A dissertation thesis submitted in partial fulfillment of
the requirements for the degree of

DOCTOR OF PHILOSOPHY

Washington State University
College of Business

August 2008

To the Faculty of Washington State University:

The members of the Committee appointed to examine the dissertation of SUTIRTHA CHATTERJEE find it satisfactory and recommend that it be accepted.

_____

Dr. Joseph S. Valacich (Chair)

_____

Dr. Mark A. Fuller

_____

Dr. Suprateek Sarker

_____

Dr. Craig D. Parks

Unethical Behavior Using Information Technology

Abstract

By Sutirtha Chatterjee
Washington State University
August 2008

Chair: Joseph S. Valacich

The aim of this dissertation is to theoretically develop and empirically test a model predicting unethical use of IT. The arguments are based on the Theory of Planned Behavior (TPB), philosophy of ethics, and economics of unethical behavior. Furthermore, this work aims to understand how technology influences this unethical use of IT.

At a broad level, this work incorporates the meta-framework provided by TPB and argues that attitude and subjective norms toward unethically using IT are strong predictors of intention of unethically using IT. Attitude is strongly influenced by ethical beliefs of the individual (drawing from the philosophical perspectives) and moral intensity of the act (of unethically using IT). Unethical use of IT is strongly predicted by intention to unethically use IT. Furthermore, unethical usage of IT is seen as an example of opportunistic behavior and this work examines as to how technology itself may provide facilitating conditions of such opportunistic behavior, thus influencing the intention to indulge in such behavior. Overall, this work examines unethical use of IT from philosophical (typically this is at an individual level), social, and technological angles and blends these considerations into a general theoretical model that can be empirically tested.

A case-scenario based empirical study was conducted in order to test for the hypotheses. The subjects were undergraduate students in a large introductory Information Systems class. The subjects were randomly assigned a case scenario describing an example of unethical use of IT and answered a questionnaire based on the case scenario. In addition, the subjects were asked questions regarding their own personal opinions in certain matters of unethical use of IT. The results of the empirical study show a significant amount of convergence with the hypotheses posited. The findings reveal that unethical use of IT is determined by individual factors such as ethical beliefs, social factors such as subjective norms, economic factors such as overall perception of gain, and technological factors such as the facilitation afforded by the technology and individual's belief in the ability to manipulate IT. The contribution, limitation, and future implications, both in terms of research and practice, are discussed.

Table of Contents

Chapter 1 - Introduction and Motivation

In today's information age, the world is progressing as a whole toward a large-scale adoption of Information Technology (IT). Computers have pervaded our daily existence. However, such widespread use of IT in every sphere of life has given rise to concerns about the use of IT for unethical purposes. With easy access to technology and the advent of the Internet, the possibility and frequency of using technology for unethical purposes has increased. Problems of software piracy, hacking, spoofing, and plagiarism have become major concerns in recent years. Some examples illustrate the point here. Business Software Alliance (2008) stated that the global piracy rate was close to 38 percent in 2007. According to them, the median piracy rate in 2007 was 61%, implying that in half the countries they studied, the piracy rate was greater than or equal to 61%. Even more concerning is the observation by BSA that, the piracy rate is 80% or higher in one quarter of the countries they studied.

The CSI/FBI computer crime survey reported in 2006 that virus and denial of service attacks were the two greatest sources of financial losses to organizations, followed by physical theft of IT, and proprietary information. The combined financial loss from these four categories is 74%. In 2007, the situation was even grimmer, when the companies in the CSI/FBI survey reported a doubling of the financial losses due to computer crime (from $168,000 in the previous year to $350,424). According to the Times News Network in 2007, about $2.1 million of pirated software was seized in India in 2006. All these examples show that unethical use of IT is very prevalent and growing at a rapid rate.

Recent academic works also indicate the expansion of unethical behavior using IT. For example, recent research (e.g. Gopal et al., 2006; Chiou et al., 2005; Al-Rafee and Cronan, 2006) shows evidence that digital piracy has grown to subsume music and movies, apart from the previously existing software piracy. Thus, it can be easily argued that the current world is seeing an increase in the frequency and scope of unethical behavior using IT. Sadly, the unethical use of IT is pervasive and seems to be growing as rapidly as the technology itself (Phukan and Dhillon, 2001). Moores and Dhillon (2000) mention that such unethical behavior is prevalent across countries. Research has also shown that individuals knowingly indulge in the unethical use of IT and even though there have been legislations produced in different countries to guard against such unethical behavior, it is common knowledge that few people obey such laws (Phukan and Dhillon, 2001). In fact, organizational employees believe that unethical IT use could lead to business success (Davis and Vitell, 1992).

However, for such a serious and potentially damaging concern, the IS literature has been largely silent. Testimony to this fact is that, over the last ten years, with the exception of a few instances (e.g. Loch and Conger, 1996; Banerjee et al., 1998; Thong and Yap, 1998; Peace et al., 2003; Limayem et al., 2004; Moores and Chang, 2006), hardly any of the studies in top IS journals have tried to shed some light on this growing, yet complex problem. A review of the top IS journals reveals a further significant observation that hardly any published study has tried to systematically develop a general model of unethical IT use (with the possible exception of Banerjee et al. (1998) and a subsequent investigation by Leonard and Cronan (2001)). Even though models of unethical behavior exist in other areas of research such as marketing (e.g. Hunt and

Vitell, 1986), till date there have been very limited attempts to develop a general theoretical understanding of unethical behavior, particularly related to the IT realm. Most of the existing studies in the IS field have taken an either an instantiation approach (mostly software piracy) or considered a narrower set of factors (e.g. software cost). Thus, we are yet to gain a general understanding of this phenomenon that represents itself as a growing worldwide problem.

Apart from the lack of general treatment of this phenomenon, a review of the relevant literature reveals that one other aspect that has been continually ignored is an understanding of this phenomenon based on the philosophical theories of ethics. Hardly any of the studies investigating possible instances of such unethical behavior draw from this rich discipline, in effect indicating a significant gap in the current literature on understanding unethical IT use. Furthermore, a review of the existing literature suggests that the role of technology in promoting such unethical behavior has practically gone unnoticed. Given that such unethical use of IT is a major concern in the IS field, the overlooking of the role of technology in perpetrating such unethical behavior seems to be a serious gap.

To summarize the concerns about previous research on this phenomenon, we find the following significant gaps in the existing literature addressing unethical usage of IT:

1. Hardly any attempt at general theorization about this phenomenon.
2. A lack of understanding of this phenomenon based on the philosophical theories of ethics
3. Hardly any attempt to unearth the role of technology itself in purporting this unethical behavior

These existing gaps enable us to argue that unethical use of IT is a phenomenon that has consistently been *under-represented* and *under-conceptualized* in the existing IS literature. Especially, we have a very narrow understanding of the factors that drive individuals to unethically use IT. This research aims to address these gaps.

The research question can thus be formally stated as: *What factors influence individuals to use IT unethically*?

In answering this question, the research draws on ethical (at an individual level), social, technological, and economic factors in order to predict the unethical use of IT.

We should acknowledge in here that there is a fertile area of research related to ethical issues of IT. However, we should take time in here to point out the key attributes of our research that differentiate it from previous work in this arena. Many have used the term Computer Ethics (e.g. Moor, 1985; Bynum, 2001) or Information Ethics (Floridi, 2002) in order to forward this line of research. However, the focus of such works, to a large extent, has been to understand the moral implications of technology (Moor, 2001), to understand how information objects can have moral properties (Floridi, 2002), and if the field of Computer (or Information) Ethics is a legitimate field of inquiry (e.g. Tavani, 2001). Furthermore, the notion of value sensitive design (e.g. Friedman et al., 2006; Friedman and Nissenbaum, 1996; Chatterjee et al., forthcoming) has illustrated how ethical values may be incorporated within a design of information systems. On a similar note, the role of ethics in Information Systems Development has been investigated by researchers (e.g. Rogerson et al., 2000; Gotterbarn, 2001). This research has a somewhat different scope: while such previous works have often tried to understand the moral nature and scope of technology and its implications in design, this research tries to

identify *the individual, social, technological, and economic factors that result in unethical use of IT*.

Structure of Dissertation

The structure of the dissertation is presented below. In this first chapter, we have introduced the topic and provided a motivation of this research. In the next chapter, we shall discuss the importance of this research and highlight as to why we need to undertake this research. Following which, we shall discuss the theoretical background. After that, we shall develop the research model and hypotheses. Following that we present our research methodology. After that we present our data analyses and the results. Finally, we discuss the results and its implications and end with the contribution and future research implications. The entire structure of the dissertation is presented below.

Chapter #	Chapter Description
Chapter 1	Introduction and motivation; dissertation structure
Chapter 2	Importance of this research
Chapter 3	Theoretical Background
Chapter 4	Research model and hypotheses
Chapter 5	Research methodology
Chapter 6	Data analyses results
Chapter 7	Discussion and limitations
Chapter 8	Contribution and Future Research

Table 1-1. Dissertation Structure

Chapter 2 - Importance of this Research

The academic importance of this work stems from multiple perspectives. First, it is a general theoretical treatment about the phenomenon of unethically using IT and brings in diverse theoretical perspectives (ethical, social, technological and economic) to explain this phenomenon. Such a diverse, yet integrative perspective has been previously missing in the literature. This research blends in philosophical (theories of ethics) and rationalist considerations (from economics) that have so far not been integrated into a comprehensive theoretical model to explain unethical use of IT.

The second important aspect of this research is that it has significant implications for IS security. This research tries to understand unethical behavior and this has a strong security angle due to the fact that it can be easily adapted for use within an organizational context. It should be noted that while the empirical study of this model is confined to students, these students are, nonetheless budding IS professionals. The behavioral nature of this model enables us to understand the relevance of factors that drive unethical behavior and it has serious implications for individuals in an IS profession. This is because unethical behavior by employees within an organization is one of the prime causes to threats to IS security. Especially professional ethics of IS professionals (in order to make use IT in an ethical manner) become an important consideration (Nissenbaum, 2004). As Johnson (1994) points out, “when one acts as a professional, one does not cease to be a moral agent” (p. 39). As a case in point, “an issue related to an employee being trustworthy is more relevant to maintaining IS security in the organization as opposed to, say in, ensuring the security of a business to consumer transaction” (Dhillon and Torkzadeh, 2006). Additionally, as Straub and Welke (1998) note, a prime threat to

security occurs from disgruntled employees and even ex-employees. They cite Neumann (1994) who mentions the case of insider currency manipulations that cost Volkswagen $260 million. As Schultz (2002) mentions, we have achieved little understanding of the "insider threat" to organziations. Garfinkel et al. (2002) actually devise a privacy protection technique to guard against insider threat, thus in effect highlighting the concern that a core area of threats of an organziation are due to the unethical behaviors of employees within such organizations. To finally reinforce our argument about the importance of studying reasons for unethical use of IT as a core concern of business organzational security, we can draw upon Dhillon and Backhouse (2000) and their views of IT security problems and challenges:

"The vast majority of breaches of systems security come from existing employees. Pressures can change individuals; marital, financial, medical problems can all play their part, sometimes in combination. Office romances are common backdrops for internal computer frauds; money is useful to impress or to keep two households going." (p. 127). Given that security concerns have a strong behavioral root, it is appropriate that we develop a model of unethical use of IT in order to shed more light on this important security concern.

Third, a specific contribution of this work, apart from its integration of diverse perspectives, is its important focus on the philosophical theories of ethics. A strong philosophical base is currently missing in IS research on this phenomena. In fact, there have been calls (Siponen and Oinas-Kukkonen, 2007) to delve more into the philosophical underpinnings of unethical IT use and this work achieves that to a great extent.

Fourth, one of the aims of this work is to initiate an academic dialogue on the nature of IS ethics (through an explication of philosophical, social, technological and economic considerations), an area which has seen limited exposure in top IS journals till date. It contributes toward a greater understanding of IS ethics, through its integration of these diverse perspectives. It also calls for more research in this area, both in continuation of this work and also to better define the scope and boundaries of IS ethics.

This work also has the potential for important practical implications. For example, if individual philosophical factors were empirically found to be strong predictors, it would imply the need for better moral education to stem the concerns of unethical use of IT. If technological and social considerations were empirically found to be more influential, then we would probably need better technological and social controls. Overall, the empirical results of this extended and diverse model would hold strong implications for practical considerations to stem the unethical usage of IT.

Apart from the above, the importance of this research stems from the fact as to how this is different from previous works in the arena of ethics and IT. As argued before, a core focus of research in this area has been to understand the moral implications of technology (Moor, 2001), to understand how information objects can have moral properties (Floridi, 1999), if the field of Computer (or Information) Ethics is a legitimate field of inquiry (e.g. Tavani, 2001), if ethical values can be incorporated in the design of Information Systems, (Friedman et al., 2006; Friedman and Nissenbaum, 1996), and Information Systems can be designed in an ethical manner (e.g. Rogerson et al., 2000; Gotterbarn, 2001). On the other hand, this research tries to find out as to *what socio-technical factors result in the improper appropriation of technology that is available*. As

Moor (1985; 2001) mentions, any technology is “logically malleable” in that it can be appropriated for a variety of purposes. Naturally, this offers the scope of the misappropriation of such technology. As a case in point, Spinello (2002) argues, “it appears easier to misappropriate intellectual property in the virtual world (of the Internet) where opportunities abound and detection is difficult” (p.23). Given that it is humans within a context that misappropriate technology in this manner, it becomes relevant to understand the human, social, and technological factors that give rise to such misappropriation.

Chapter 3 - Theoretical Background

In this section, we review literature that is appropriate for the development of our theoretical model. They are the philosophical theories of ethics, the theory of planned behavior (TPB), and the economics of unethical behavior (especially Transaction Cost Economics or TCE). First, we need to justify as to why we think that these streams of literature are important. Unethical use of IT by definition incorporates the notion of ethicality. Knowledge of the philosophical theories of ethics thus guides our understanding in this regard. Then, the TPB is a powerful framework to understand human behavior that stem from attitudes and intentions. Since unethical use of IT is a behavior, we find a natural relevance of the TPB framework to our research cause. Finally, a major reason of unethical use is economic benefits. If unethical behavior did not produce any economic benefits (actual or perceived), then there would be no rationale to indulge in that behavior. Hence economic theories (such as TCE) are a natural source to gain a deeper understanding as to why people behave unethically using IT and how perceived economic benefits may explain unethical use of IT.

Philosophical Theories of Ethics

Philosophical theories of ethics can be classified into two major categories: the consequentialist school and the deontological school (Smith, 2002)[1]. The consequentialist school views that the rightness (or wrongness) of an action (behavior) is determined by how much consequential benefit (or loss) comes out of the action. Early proponents of the consequential school of thought were Bentham (1789) and Mill (1861).

[1] There is a third stream of ethical thought called virtue ethics which we discuss later in this dissertation

The early notion of utilitarianism (the most prominent stream of thought within consequentialism) proposed by Bentham and Mill viewed that any action should be judged as ethical accordingly as it maximizes pleasure and minimizes pain. However Moore (1903) deviated from such an idea of purely hedonistic consideration, and proposed his version of ideal utilitarianism, which advocated judgment of an ethical act by non-hedonistic consequences such as material benefits.

On the other hand, the deontological school of ethics views that rightness or wrongness of an act is determined by certain rules in place. Probably the most well known of the philosophers within the deontological school of thought is Immanuel Kant who grounded these rules in the form of his famous categorical imperatives:

1. "Act only according to that maxim whereby you can at the same time will that it should become a universal law" (Kant, 1804/1994: 30).
2. "Act in such a way that you treat humanity, whether in your own person or in the person of another, always at the same time as an end and never simply as a means" (Kant, 1804/1994: 36)
3. "Every rational being must so act as if he were through his maxim always a legislating member in the universal kingdom of ends" (Kant, 1804/1994: 43).

Each of these categorical imperatives represents "an action as objectively necessary in itself, without reference to another end" (Kant, 1804/1994: 25). Any such objectively necessary action represents a rule and it is the individual's duty to follow the rule. For example, it is objectively necessary to speak the truth and hence it would be incorrect to lie under any circumstances. This is because, according to Kant, if one were

to tell a lie, then it should universalized (the first categorical imperative) and then there would be no need to lie at all (since everybody would be lying, it would defeat the very purpose of lying). Thus, lying lends itself to a contradiction as per the first categorical imperative and hence should never be done. In short, Kant's deontological view is that any action is ethical if it conforms to certain rules (e.g. do not lie; do not kill; do not cheat) that follow logically from the categorical imperatives.

Notwithstanding the vast amount of philosophical and practical discussions that these theories have spawned, they are not above criticism. Both deontology and consequentialism can be criticized on many grounds. For example, a common and potentially serious criticism of consequentialism (e.g., Anscombe, 1958) is that it does not provide any guidelines on how we should act. In consequentialism, morality is based on consequences, and these are difficult to determine *a priori*. Within this perspective, the ethicality of an act can only be judged as ethical or unethical *post hoc*, and no guideline is available for acting in a manner that is indubitably moral, making consequentialism somewhat impractical (Singer, 1977; Lenman, 2000). In addition, consequentialism has also been criticized because consequentialism can be used to justify human atrocities such as war, slavery, mass killings, or murder (Nagel, 1988). For example, if killing an innocent person made a lot of people happy, then consequentialism would advocate it. The consequentialist view does not acknowledge the existence of individual rights that are sacred, such as the right to life. Critics argue that if this view is perpetrated, then the whole world could descend into anarchy of murder and mass killings. In summary, the problem with consequentialism is that harm to an individual can always be justified by a gain for others. As Waldron (1995) mentions, according to

utilitarianism (the most prominent stream of consequentialist thought), there is "nothing intrinsically wrong with sacrificing an important individual interest to a greater sum of lesser interests."

Again, both deontology and consequentialism represent the "universalist" view of ethics- that is they provide abstract universal principles in order to undertake any ethical analysis. Many of the classical and twentieth century ethicists subscribe to this notion of ethics, where the human being is supposed to be the free, detached rational agent with objective thought processes, and is guided by universal paradigms that decide on the moral course of action (Yuthas and Dillard, 1999). The primary aim of these universalist perspectives is to understand as to how universalized principles can be derived and implemented (Markel, 1997), such that any ethical analysis can be undertaken. However, the basic problem with such universal notions is that the application of such universal principles again implies an objective measure of reality, where the knowledge is separate from the reality and is neutral. As a result, these theories have often been criticized by many recent philosophers (e.g. Hursthouse, 1999; O'Neill, 1996; Taylor, 1985; Sandel, 1982; MacIntyre, 1985) due to their preoccupation with such universal principles, which, they say, prescribes abstract thinking and uniform treatment (Hursthouse, 1999) regarding ethicality. They argue that universal theories of ethics present an overtly idealized view of the reality, for example, especially overlooking the embeddedness of the human beings within particular situations and contexts, and ignoring the fact that they do not account for human emotions and moral impulses (Bauman, 1993; MacIntyre, 1985). Due to the universalist perspectives being impersonal and neutral, they provide an incomplete view of human nature (Whetstone, 2001), and consequently of socio-technical

phenomena such as unethical IT use. The point of the above example is to highlight a *significant* shortcoming of such universal perspectives of ethicality. Employing such universal perspectives takes away the primary *moral responsibility* from the individual because they equate ethicality with rationality (Stahl, 2008). Further, universal moral theories also suffer from two shortcomings which, ironically, are due to their overtly rational and objective stance (Donaldson and Dunfee, 1994): a) the inherent bounded moral rationality of the agent, and b) the inability of universal moral theory to account for commonsense moral convictions and individual preferences. The first one refers to the fact that no matter how informed or rational the moral agent is, human beings have a finite set of intellectual resources and are inherently bounded by it (Simon, 1956). This bounded moral rationality is one of the pitfalls of the universal theories of ethical analysis. It is certain that the moral agent would err in applying the theories across situations, due to their (the agent's) inherent boundedness.

The other problem is that the moral theories, themselves, will err on this ground. The moral theories, in their quest for objectivity and neutrality, are *unable* to account for *individual moral convictions, and impulses.* The present world is infinitely complex and the entire panorama of situations and contexts are huge, so that any universalism cannot be readily applied across such contexts and situations. Thus, both the universal principles and their appliers (the rational agents) fall short when undergoing an ethical analysis of any situation.

In spite of these criticisms, both these theories are strong schools of ethical thought and hence they are still appropriate in an ethical analysis of the situation. One important argument in their favor is that they are both universal, act-based schools of

ethics. Thus, they are both essentially very amenable to behavioral understandings of human beings on a broad (universal) level, which is the focus of this research.

The Theory of Planned Behavior

The theory of planned behavior (Ajzen, 1991; Beck and Ajzen, 1991) asserts that actual behavior is influenced to a great extent by the intention to carry out that behavior. The intention to carry out any behavior is influenced by the attitude toward the behavior, the perceived behavioral control of the user, and the subjective norms toward the behavior. The perceived behavioral control of the user is the user's perception about the ability to carry out an act. The subjective norms imply the pressures from the social environment. At a very basic level, they can be understood to be the acceptability of an act (of an individual) by people surrounding the individual (e.g. peers, friends, authorities etc).

TPB has been validated empirically across various contexts. Armitage and Conner (2001) found that the TPB predictions held over 185 studies in various domains. Thus, it can be concluded that the TPB is a powerful theoretical framework for predicting human intentions and behavior. This is one key reason why we chose to base our theoretical model of unethical use of IT (a behavior) on TPB. Our use of TPB as a theoretical anchor finds justification in the following words of Armitage and Conner (2001):

"The present meta-analysis provides support for the efficacy of the TPB as a predictor of intentions and behavior. Although prediction is superior for self-reported than observed behavior, the TPB is still capable of explaining 20% of the variance in prospective measures of actual behavior (i.e. a medium to large effect size). The present findings therefore corroborate those of previous TPB meta-analyses…The present study

showed that PBC independently predicted intentions and behavior in a wide number of domains…Finally, work on additional normative variables (e.g. moral or descriptive norms) may increase the predictive power of the normative component of the model" (p. 489)

It should be noted that this work actually calls for the inclusion of moral norms toward extending TPB work. Inspired by this perspective, we introduce ethical factors into the TPB framework in order to explain the phenomenon of unethical use of IT.

Economics of Unethical IT use

Transaction Cost Economics (Williamson, 1975; 1981; 1985) tries to understand the reasons behind the breakdown of market governance and the establishment of hierarchies to exercise control over economic transactions. Transaction cost economics has been readily applied from marriage to international trade to sociology to organization theory and many more such arenas (Rindfleisch and Heide, 1997). The unit of analysis in Transaction Cost Economics (TCE) is a transaction. One of the major interests of TCE is to understand what conditions and mechanisms facilitate a transaction. While at first sight, TCE seems an inappropriate base as it has been mainly applied at the organizational and institutional level, on closer scrutiny, we can argue that the basic tenets of TCE apply equally at the individual level and also to non-market situations (e.g. Treas, 1993). In fact as Williamson (1985) notes, "Any problem that can be formulated, directly, or indirectly, as a contracting problem can be investigated to advantage in transaction cost terms" (p. ix). If we understand unethical IT use as a violation of a social contract between individuals and society (or even the organizations they work in), we can

see how TCE becomes an important theoretical guide on which to base our arguments. Inherent in its nature, unethical use of IT has the considerations of costs both for and against the behavior, making TCE a relevant theoretical lens. Furthermore, even though TCE has been mostly applied at the organizational and institutional level, the basic assumptions on which transaction cost analysis (TCA) is based are universal human attributes: opportunism, bounded rationality and risk neutrality (Rindfleisch and Heide, 1997).

Of the three assumptions of TCE, we find that the universal human attribute of opportunism becomes especially relevant to our discussions and arguments presented in this research. Opportunism is the assumption that if decision makers are provided with the opportunity, they may unscrupulously seek their own interests (Rindfleisch and Heide, 1997). Williamson (1985) defined opportunism as "self interest seeking with guile" and argued that it includes such behaviors as lying and cheating. Opportunism is a fundamental assumption of human nature according to Williamson (Ghoshal and Moran, 1996) and could be controlled by having proper safeguards and controls (Williamson, 1993).

The concept of opportunism thus has a strong link with unethical behavior. Unethical use of IT can very well be framed as a case of opportunism. As we shall see later on, the concept of opportunism provides an important lens through which we can understand the individual's intention to use IT unethically, especially in the presence (or absence) of existing sanctions and controls.

Before we end this literature review of TCE, we should point out the fact that our aim was not to dwell on a systematic review of TCE. This would be an independent study

by itself. Rather, our idea was to extract, through this review, an important concept (opportunism) of the TCE that becomes very relevant to this research. We aim to use this key idea in order to develop and reinforce our theoretical arguments presented later.

Chapter 4 - Research Model and Hypotheses Development

Arguing from the above theoretical base, this section tries to develop the research model explaining unethical IT use. Before that, we should showcase the entire conceptual model based on the TPB.

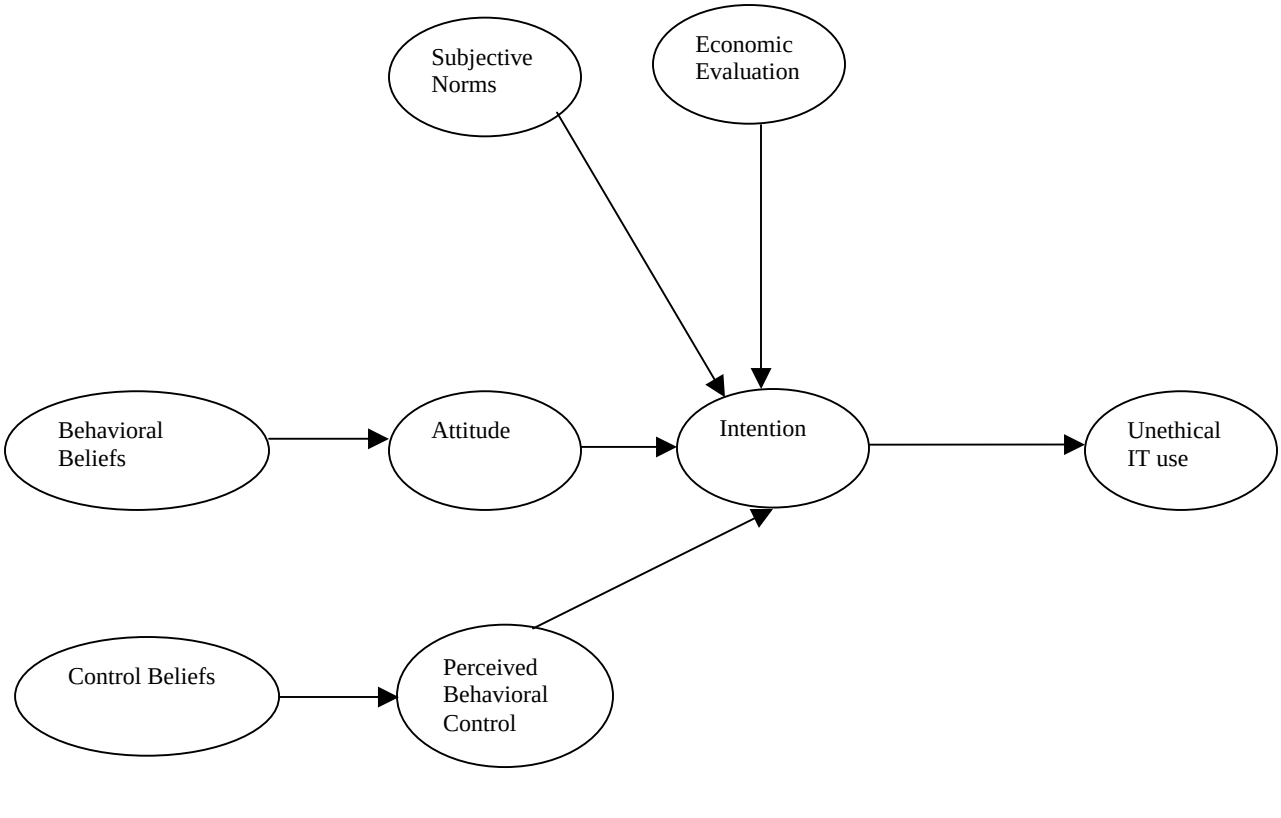

Figure 4-1. The conceptual model based on the TPB

The conceptual model, as shown above, draws from the TPB where intentions of an act are influenced by the attitude toward the act, the perceived behavioral control for the act and the subjective norms toward the act. Each of these predictors, in turn, is influenced

by various beliefs, such as behavioral beliefs, and control beliefs respectively. Additionally, perceived behavioral control also influences intention to perform that behavior. In addition to the conceptual structure provided by the TPB, an additional contingency of economic evaluation is introduced. As the TPB is primarily a socio-cognitive model (Armitage and Conner, 2001), and thus does not have an explicit rational evaluation of costs and benefits, we find it appropriate to introduce this perspective within the scope of our conceptual model.

However, in our conceptualization, we opted to exclude the normative belief (as a predictor of subjective norms) component out of our theorization. There are two reasons for this. First, as Armitage and Conner (2001) argue, normative belief components are indeed strong predictors of intentions and both subjective norms and normative beliefs correlate strongly with each other. Hence, a decision was taken to include only the subjective norm component in the research model. Second, given that this is an IS research, social antecedents of subjective norms are deemed much less important.

Having articulated this overall conceptual model, we now proceed to develop and present our research model. The entire research model is shown in Figure 4-2.

Unethical IT use

An act, in general, is defined to be unethical when "one party, in pursuit of its goals, engages in a behavior that is harmful to the abilities for other parties to pursue their goals" (Kuo and Hsu, 2001). Mason (1986) defined *privacy*, *accuracy*, *property* and *access* (henceforth PAPA) as four ethical issues of the information age.

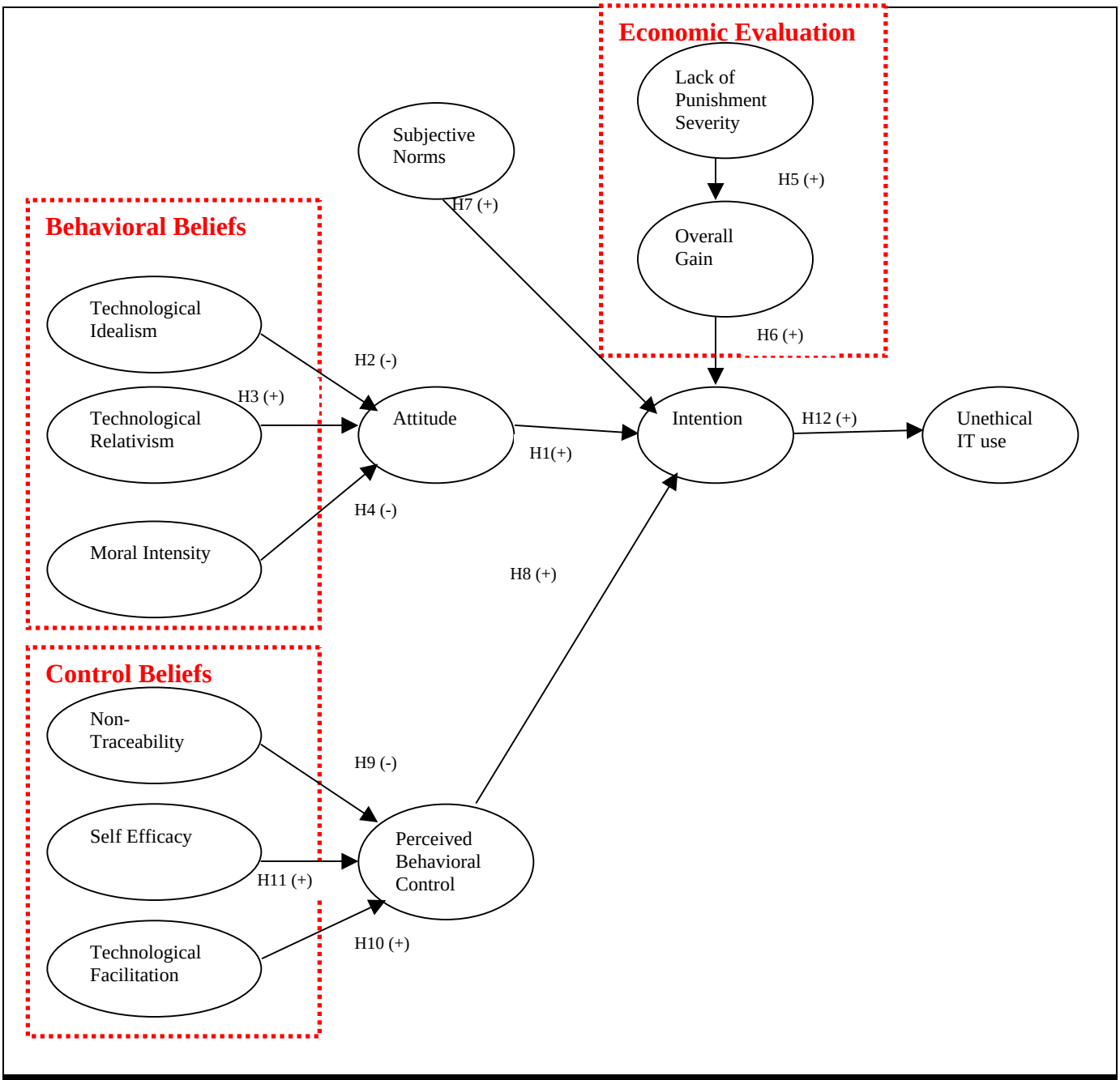

Figure 4-2. The research model

In line with the views of Mason (1986), and adapting Chatterjee's conception of unethical behavior (2007), we *define unethical use of IT as the violation of privacy, property, accuracy and access of any individual, group or organization by any other individual, group or organization*. It should be noted that the commonly known forms of unethical IT use such as software piracy, hacking, spoofing, plagiarism etc. all fall within the scope of this definition. This research considers the violator to be an individual.

Attitude Toward Unethical Use of IT

Fishbein and Ajzen (1975) define attitude toward an act as the degree to which a person is favorable or unfavorable about the act. In our case, attitude toward unethical IT use is defined as the degree of favorableness toward the violation of PAPA for any other individual, group or organization. According to the Theory of Planned Behavior (Ajzen 1991), attitudes are strong predictors of intention, and thus we can argue that a strong attitude in favor of unethical use of IT would lead to a greater intention about unethical use of IT. Hence we hypothesize:

H1. Attitude in favor of unethical IT use would positively influence intention in favor of unethical IT use.

Beliefs about Information Technology

Any ethical attitude is influenced by the ethical fairness or justness of the action and entails a judgment regarding the basic ethicality of an act (Reidenbach and Robin, 1990; Ellis and Griffith, 2001). Our theoretical foundation of TPB is consistent with this

position, and suggests that human beings' attitude toward an action is driven by certain beliefs about the action. Thus, in our case, we argue that the attitude toward using IT unethically is strongly influenced by certain ethical beliefs.

But what are those ethical beliefs, and what do they pertain to? Drawing upon existing research, we can argue that there are three kinds of ethical beliefs that are important antecedents in the formation of attitude toward using IT unethically: technological idealism, technological relativism and moral intensity.

The literature on ethical beliefs (e.g. Forsyth, 1980; 1981) argues that ethical beliefs of human beings are governed by two distinct concepts which are essentially orthogonal to each other: idealism and relativism. The concept of technological idealism draws from Forsyth's (1980) concept of idealism as a predominant stream of individual ethical belief influencing the attitude regarding any moral issue. Idealism is defined as the belief that one should not harm others (Forsyth, 1980). Adapting this notion, we define technological idealism as an individual's belief that IT should not be used in order to harm anyone. The reason for our adaptation is that we feel that since our scope of investigation is unethical use of IT, ethical technology related beliefs are more relevant within our scope of investigation. Inherently, as is evident in its definition, technological idealism draws upon a consequential perspective about technology, and is informed by the notion that any technology related action should maximize the (good) consequences. Unethically using IT has the increasing possibility of causing harm to the victim. As a case in point, each of the unethical behaviors, like hacking, digital piracy, etc affect an individual, group, or organization in some way or the other. For example, digital piracy affects revenues of organizations. Hence, an individual who subscribes to the belief that

technology should not be used in order to harm others, would develop less degrees of favorableness (attitude) toward unethically using IT. Hence, we can argue that individuals having a high level of technological idealism would tend to have a negative attitude toward unethical use of IT. Hence, we have:

H2. Technological idealism would negatively influence attitude in favor of unethical IT use.

Drawing upon Forsyth's work again, we note that relativism is the notion that individuals would not appeal to a uniform code of moral conduct in order to develop a moral attitude toward any ethical action. Instantiating the notion of relativism in the context of our work, we can define technological relativism as an individual's position that using technology should not conform to any codes or rules in place. Individuals who rate higher on technological relativism do not believe in abiding by rules (or codes) in place, and thus determine an act as ethical based on its situational context (Reidenbach and Robin, 1990; Trevino, 1986). For example, studies have found that ethical acceptability of the same act is different across different cultures (e.g. Husted, 2000). On the other hand, lower relativists are staunch deontologists who believe that technology should be used in such a way that conforms to various rules in place. For example, they would expect that the ACM Codes of Ethics should be strictly followed, irrespective of the situation. Thus, we can argue that staunch deontologists, subscribing to rule-based ethical conduct (Ellis and Griffith, 2001; Reidenbach and Robin, 1990; Reidenbach et al., 1991), would have significantly lower levels of favorableness regarding the use IT in ways inconsistent with the ACM Code of Ethics. Conversely, we can thus argue that individuals who are not staunch deontologists (i.e. who are high on

technological relativism, (and thus determine if an acts unethical based on the surrounding context) are much more likely to have a positive attitude toward using IT in ways that may be seen as unequivocally unethical by deontologists. Hence we can hypothesize:

H3. Technological relativism would positively influence attitude in favor of unethical IT use.

Moral Intensity

However, beliefs about how technology should be used should not be the only concern during attitude formation about unethically using IT. The literature has also considered the moral intensity as an extremely important factor in ethical decision-making (Jones, 1991). Moral intensity refers to the fact that the characteristics of the issue at hand influence our ethical decision making process (Jones, 1991). It is defined as the "extent of issue-related moral imperative in a situation" (Jones, 1991:372). For example, as Singhapakdi et al. (1996) argue, if the moral intensity of a situation is perceived as low, individuals will not view the situation as having an ethical component. For example, changing an individual's medical dosage electronically has a significantly high level of moral intensity than, for example, copying pirated software from a peer. Based on prior literature (e.g. Singhapakdi et al., 1999), we can say that a high moral intensity of an unethical IT use would significantly lower the degree of favorableness of an act of unethically using IT. Hence, we can hypothesize:

H4. Moral intensity would negatively influence attitude in favor of unethical IT use.

Lack of Punishment Severity

Unethically using IT (in order to serve one's own interests) is clearly a case of opportunism, as argued before. Literature has argued that opportunistic behavior is positively influenced by the benefits from the behavior (Riordan and Williamson, 1985) and is negatively influenced to the sanctions that are in place for that behavior (Ghoshal and Moran, 1996).

In other words, the overall gain perceptions from committing an act is positively influenced by the perceived lack of repercussions for the act. Punishment for an unethical act is such a repercussion. Overall gain of committing any act can be understood to be a cost benefit analysis. In case of unethical acts such as unethical use of IT, thus, the overall gain perceptions of human beings are positively affected by the individual's perceptions of lesser punishment for that act. Thus, lack of punishment severity should have a strong positive influence on an individual's perceptions of committing an act. Thus, we hypothesize:

H5. Perceived lack of punishment severity for unethical IT use would positively influence perceptions of overall gain from unethical IT use.

Overall gain

As argued above, unethical use of IT is clearly a case of opportunism and hence human considerations of overall gain from committing the act become an important consideration. In fact, as McPhetters (1976) notes, criminal behavior has often been

studied from a rational angle which factors in how much of overall gain individuals perceive from a certain behavior.

The reasoning behind this argument is the fact that according to the economic line of thought, human beings essentially are geared toward maximizing their self interest. As Sen (1977) notes, the entire stream of economic research has presupposed that human beings are guided by self-interest and act accordingly so as to pursue their overall interests. In other words, human beings are essentially rationalists, however bounded they might be (Simon, 1956), and inherently try to maximize their gain. It has been shown in past research that perceptions of overall rewards (from committing the unethical behavior) encourage individuals to engage in unethical behavior (Schweitzer et al., 2004).

According to TCE and Williamson's model of unethical behavior, we can argue that opportunistic behavior shall be undertaken if the overall gain from behavior (for whatever reasons, e.g. due to the existence of low sanctions) is high. Such an argument is also reflected in the expected utility theory (Savage, 1954; Schoemaker, 1982) that posits that individuals would weigh the alternatives against each other and that the alternative with the best outcome would be selected. In essence, the individual would undertake a cost-benefit analysis for each alternative and accept the alternative that would maximize the utility (Peace et al., 2003).

So, an option that represents an overall gain, increase an individual's intention of behaving unethically. The costs could be sanctions in terms of financial penalty or jail time (Peace et al., 2003). Consistent with TCE, this would imply that individuals would have a higher intention of committing an act if the act had a high level of overall gain

associated with it. Consequently, they would have a greater degree of intention to carry out the act. Putting the act in our context of unethical IT use, we can hypothesize:

H6. Perceived overall gain from unethical IT use would positively influence intention in favor of unethical IT use.

Subjective Norms

We have thus far discussed ethical judgment with respect to attitude resulting from the individual ethical philosophy which draws from the universal notions of act based ethicality. Both the consequentialist and deontological theories represent these universal, act-based universal theories of ethics. They represent the view that the rightness and wrongness of action can be understood from universal principles of either rule-based or consequence-based actions. Unfortunately, as mentioned before, these classic theories have come under scrutiny from recent philosophers (e.g. Hursthouse, 1999; O'Neill, 1996; Taylor, 1985; Sandel, 1982; MacIntyre, 1985; Bauman, 1993) due to their preoccupation with these universal principles, which, they (recent philosophers) say, overlooks the embeddedness of the individual within a particular context. They argue that surrounding contexts temper individual's notion of goodness and that essentially the notion of good is socially constructed by the community that the individual is a part of.

An important concept that surfaces through these criticisms of deontology and consequentialism is that of guidelines, requirements, and parameters inherent in a social system (Reidenbach and Robin, 1990). This social dimension of ethical judgment judges an act as ethical according to its social acceptability. Thus, social judgments about an act can vary across social cultures (Trevino, 1986). Studies have found that cultural

acceptability of the same act is different across cultures (e.g. Husted, 1999; 2000). Hunt and Vitell (1986) and Ferrel and Gresham (1985) argue that society has an influence whether we actually intend to perform an act.

The TPB nicely factors in this concept of social conformation through the construct of subjective norms. Kuo and Hsu (2001) define subjective norms as "desire to conform to others: confirm what others do, do what others do." Subjective Norms refer to the social evaluation of the behavior by the individual. While attitudes are primarily predispositions (Zimbardo, 1970), subjective norms vary by the reference group and represent the contextual understanding of ethicality. As argued above, subjective norms can be understood to be the acceptability of an act (of an individual) by people surrounding the individual (e.g. peers, friends, authorities etc). Thus, an individual moving from one context to another would be subject to different subjective norms, but would retain the individual level of ethical judgment (represented by technological idealism and relativism).

Again, according to the TPB, subjective norms are strong predictors of behavioral intention. Adapting to our context, we can thus hypothesize:

H7. Subjective norms toward unethical IT use would positively influence intention in favor of unethical IT use.

Perceived Behavioral Control

The theory of planned behavior or TPB (Ajzen, 1991; Beck and Ajzen, 1991) posits that the perceived behavioral control of an act is an important consideration in the ultimate carrying out of an act. The perceived behavioral control of the user is the user's perception about the ability to carry out an act (Ajzen, 1991). TPB posits that in order to

intend and carry out an act, a user should also perceive that s/he has the capability to carry out that act. Empirically, perceived behavioral control of software piracy (a typical case of unethical IT use) has been shown to positively influence intentions of software piracy (Peace et al., 2003). Based on these arguments, we can propose that a higher perceived behavioral control in carrying out an unethical act would influence the intention of unethical act. After all, if an individual does not perceive that carrying out an unethical act would be within his/her control, s/he would never intend to do it. Hence, we hypothesize:

H8. Perceived Behavioral control of Unethical IT use would positively influence intention in favor of unethical IT use.

Influences of Technology on unethical behavior

In this section we describe how technology by itself can influence unethical behavior. We first emphasize and justify our argument that technology can by itself facilitate unethical behavior and then develop our hypotheses related to the effect of IT on unethical behavior.

As we emphasized in the past sections, there are various different considerations in unethical use of IT. However, our argument is also that *technology itself could have certain characteristics that can help an individual behave unethically*. Consequently, if we are to understand unethical behavior using IT, we should understand the behavioral control that technology provides so as to aid in this unethical behavior. An understanding of technology-induced unethical behavior can actually facilitate considerations for designing better technology so as to reduce this unethical behavior using technology.

Herein, we justify and understand the notion as to how technology can induce unethical behavior before developing our hypotheses related to technology-induced unethical behavior.

It has been previously argued that technology may have introduced newer ethical problems due to the very nature of technology and that it has the ability to influence unethical behavior (Marshall, 1999; Tavani, 2001; Chatterjee, 2007). For example, Marrett (2004) and Capel and Windsor (2000) argue that technology provides an environment for unethical acts. Zmud (1990) argues on a similar note and mentions that technology could aid deceptive behavior. As Ellison et al. (2006) note, deceptive practices are common in online dating environments, curbed only to an extent by the fear of losing credibility during any future face-to-face interaction. Thus, we can safely argue that technology can be used as a means for deceiving others. In fact, the growing literature on deception, a typical form of unethical behavior (e.g. Zhou et al., 2004; Zhou, 2005; Grazioli and Jarvenpaa, 2003; Grazioli and Jarvenpaa, 2000), has argued that technology has created a scope for deception.

Moor (1985; 2001) argues that technology is uniquely malleable and it can be appropriated for a variety of purposes. As a case in point, Spinello (2002) points out that the Meta tag (HTML code used to provide a web page information summary) is particularly sensitive to manipulation.

Hence, it can be logically argued that technology, through its various characteristics, can facilitate unethical behavior. As Maner (1996) puts it, technology raises “ethical questions that depend on some unique property of prevailing computer technology” (p. 9). Essentially, these characteristics of technology trigger the technology

induced behavioral control related to committing an unethical behavior using technology. For example, connectivity (or network connectivity) offered by IT provides a scope of unethical use of IT. Any form of unethical IT use benefits from positive network externalities, where the marginal benefit increases with every additional element in the network. Consider this situation: If the computers across the world were just standalone and not connected, there would hardly be any case of unethical IT usage. If everyone were working on a standalone computer, the scope and possibility of unethical behavior would be greatly reduced, as by definition unethical usage of IT involves violation of PAPA and this violation would hardly be possible without any connectivity induced by the technology. The possibility and benefit of unethical IT use arise from the fact that computers across the world are interconnected. Whether it is copying or distribution of illegal software (Conner and Rumelt, 1991) or a proliferation of viruses (Householder et al., 2002) or an attack by worms (Bagchi and Udo, 2003), or even hacking into a computer network, computer crimes benefit from the facilitation offered by IT. For example, Householder et al. (2002) mention that the “Code Red Worm” virus infected more than 250,000 systems around the globe. This would not have occurred had the computers not been internetworked. Consider again the case of software piracy. Software piracy would not have been so prevalent had IT not enabled us in facilitating this behavior. Illegally downloading software would not have been possible without the internetworking. Again, distribution of such software would not have been possible without the efficiency of distribution offered and facilitated by IT.

As a final argument, we can relate back to the definition of unethical use of IT. By definition, it is the violation of privacy, property, accuracy and access of an individual,

group or organization by any other individual, group or organization. Note that this violation is certainly not possible unless one has access to the IT resources others have. The existence of IT resources and the access of such resources are artifacts of the existence of technology itself. Thus, it can be reasonably argued that IT itself perpetrates unethical behavior, especially in its unethical use.

Resource facilitation: Non-Traceability

But how does technology provide a facilitating role in perpetrating unethical behavior? One important consideration is that it provides (or does not provide) certain resources within the scope of unethical behavior. In this regard, one important resource is the availability (or not) of audit trails and logs that aim to track (or "trace") users' unethical behavior. Traceability is defined as the ability to trace an individual's action (and thus the individual) using the technology available. The lack of traceability is thus closely linked to anonymity, which has been argued to be an important implication of technology use (Johnson, 1997; Wallace, 1999). Anonymity can be defined as the non-coordinability of traits (Wallace, 1999) and the inability to determine the true identity of an individual. In other words, we cannot relate an anonymous individual with any other traits of the individual (i.e. looks, user id, social security number, phone number, address etc). This leads to the possibility of the "personal denial of responsibility" (Harrington, 1996) and this partly explains why anonymity breeds the threat of opportunism. A party who is anonymous has a greater chance of behaving opportunistically (Mandaric and Oberweis, 2002; Baron, 2002). Such an argument also finds justification in the

deindividuation literature (Zimbardo, 1970; Diener, 1980) where anonymity has been argued to be a key predictor of unethical and antisocial behavior.

So, we can argue that an individual inherently perceives that the IT provides non-traceability of his/her act, perceives more behavioral control in carrying out the act, primarily because there are no future repercussions (due to anonymity) to be worried about. Hence, we hypothesize:

H9. Perceptions of non-traceability provided by technology positively influence an individual's perceived behavioral control for unethical IT use.

Technological Facilitation

The inherent interconnected nature of IT provides certain opportunities for unethical behavior. Consider this example: If the computers across the world were just standalone and not connected, there would be fewer instances of unethical IT use. As argued before, the possibility and benefit of unethical IT use arise from the fact that computers across the world are linked, a natural feature of today's technology. Whether it is copying or distribution of illegal software (Conner and Rumelt, 1991) or a proliferation of viruses (Householder et al., 2002) or an attack by worms (Bagchi and Udo, 2003),we find that it is technology that facilitates such unethical behavior. Again, for example, indulging in software piracy is related to a great extent to the fact that the illegal copies can be efficiently made and are equivalent to the original (Conner and Rumelt, 1991). Similar is the case with viruses and other such malicious codes. Due to digitization, malicious codes can travel unchanged throughout the entire network. A copy of a virus can thus travel unchanged and every copy can be equally efficient and effective on its target. Technology, especially software code, can be favorably equated with Latour's

(1987) conception of the immutable mobile. In summary, technology can facilitate unethical behavior through its inherent properties such as efficiency and accessibility.

We can then argue that individuals who feel that the technology provides certain facilitating attributes for carrying out the unethical action would consider their behavioral control regarding the using the technology (for an unethical act) to be higher. Thus we hypothesize:

H10: Higher perception of technological facilitation for the unethical IT use would increase the perceived behavioral control for unethical IT use.

Computer Self Efficacy

Till now, we have discussed the effects of IT on unethical behavioral, by its effect on the perceived behavioral control which ultimately affects intention and behavior of an unethical act using IT. There is another aspect in which technology related factors can affect unethical IT use- the perception of the individual that s/he can really use IT for an unethical purpose.

In this line of argument, it is useful to note that Taylor and Todd (1995) decomposed perceived behavioral control and proposed that one of the key antecedents to perceived behavioral control is the general computer self-efficacy of the individual. General computer self efficacy draws from the fact that the individual is perceives himself/herself to be skilled in computers and has knowledge and familiarity with computers (Loch and Conger, 1996). Thus, arguing within our context, if an individual perceives a greater amount of self-efficacy in handling computers, then the perceived behavioral control of the unethical IT use would increase. Unethical acts using IT need

IT skill. A novice in computer technology, without sufficient confidence regarding his/her skills, cannot seriously intend to carry out an unethical act using IT, nor can s/he actually do so typically. Hence we hypothesize:

H11: Computer Self Efficacy of the individual would positively influence the perceived behavioral control for unethical IT use.

Intentions and Behavior

Finally, according to the TPB, intentions are strong predictors of actual behavior. Putting this act in the context of our unethical use of IT, we can directly hypothesize:

H12: Intention to unethically use IT would positively influence actual unethical use of IT.

Chapter 5 - Research Approach and Methodology

This chapter provides a discussion of the research approach and methodology used in this study. This chapter is structured as follows. Following the introduction, the research methodology is discussed. After that, the research measures are defined and discussed.

This study may be characterized as a positivist study where the researchers subscribed to an objective ontology. In accordance with this positivist ontology, a positivist epistemology consisting of a case-based scenario was used. The cases were manipulated in order to reflect different levels of certain exogenous variables. Thus, this study may be best understood as a quasi-experimental design. The reason is that while there were indeed manipulations presented in form of case scenarios, the nature of the study did not present any scope for control groups. Furthermore, certain other variables, most notably demographic ones (e.g. gender, socio-economic status etc) were not controlled for. We recognize that these variables in this description could have an important influence on phenomenon of interest and we urge future research to dwell on this issue further.

Sample

The research methodology consisted of a case-based study distributed to a body of undergraduate students. Case-based study has been prevalent in existing research on ethical issues related to IT (e.g. Banerjee et al., 1998; Thong and Yap, 1998; Ellis and Griffith, 2001; Leonard and Cronan, 2001; Haines and Leonard, 2007) and this research aims to follow along the same lines. In such a methodology, a number of ethical

scenarios (relevant to students) are distributed to the subjects and their responses are elicited through an administered questionnaire. While there can be concerns raised as to the relevance of student subjects in such a study, a lot of previous research, especially on software piracy issues, have used student subjects (for an extended list of such studies, please refer to Limayem et al., 2004). Also, the student body represented in this sample are themselves budding IS professionals. Essentially, through the usage of student subjects, we would get an idea of how undergraduate students in an MIS course (many of whom would embark on a career in IT later on) feel about various ethical scenarios using IT. Thus, usage of student subjects would seem reasonably appropriate for this study. We do not have any reason to believe that students would feel differently on the essential factors that this model comprises of. Factors of individual ethical philosophy, technological facilitation and net gain evaluation, should be no differently perceived by students as compared to professional employees.

To summarize, our choice of student subjects is particularly justifiable because: a) they are future organizational members, future developers and users of IT; b) there is no theoretical reason to believe that students would feel differently on the essential factors examined compared to real-world practitioners; in other words, factors associated with individual ethical philosophy, technological facilitation, and punishment would be no differently perceived by students as compared to professional employees; and c) the scenarios used are actually relevant to students. Thus, we believe that the use of student subjects is appropriate for this study.

Study Design and Ethical Scenario Cases

As mentioned above, the sample comprised of a large body of undergraduate students (enrolled in an MIS course), who were provided a specific ethical scenario (randomly), and asked to answer a questionnaire. Each case corresponded to a set of "manipulations." In order to reduce possibilities of order effects and possible fatigue, and sensitization by repeated exposure to the instrument within a single study session, each student was not assigned multiple cases.

The base scenarios comprise of two distinct unethical behaviors using IT: a) an incident of illegal downloading of music and, b) an incident of unauthorized grade change. These two scenarios were chosen because of their immediate relevance to the study sample. The two base scenarios were modified to manipulate the exogenous variables of moral intensity, technological facilitation, and punishment severity. Samples of the different case scenarios are presented in Appendix A. After removing missing data, a total of 493 usable questionnaires were available.

Instruments and Measures

All the measures (7 point Likert scale, ranging from strongly disagree to strongly agree) used were adapted from prior literature and subjected to prior pilot testing for further refinement. The following sections describe the literature sources from which the items were adapted/developed. The entire instrument showing all the items is shown in Table 5-1.

Construct	Variable	Measures for each construct
Technological Idealism (IDEAL)	IDEAL1	Individuals using Information Technology (IT) should make certain that their IT use does not intentionally harm another person even to a small degree
	IDEAL2	IT should never be used to psychologically or physically harm another person
	IDEAL3	IT should never be used to threaten the dignity and welfare of another individual
	IDEAL4	Whenever I use IT, I should be concerned about whether the way I use it maintains the dignity and concern of the society.
	IDEAL5	When I use IT, I should make certain my use does not sacrifice the welfare of others.
	IDEAL6	Moral actions using technology should match the ideals of the most "perfect" action.
Technological Relativism (RELA)	RELA1	How I use technology should not be part of any code of ethics.
	RELA2	Questions of what IT use is ethical for everyone can never be resolved since what is moral or immoral is up to the individual.
	RELA3	Morality of any IT use should be judged only on personal standards, and should not be applied to others.
	RELA4	Ethical considerations in using IT are so complex, that individuals should be allowed to formulate their own individual codes.
Attitude toward unethical IT use (ATT)	ATT1	Carrying out the action would be good.
	ATT2	Carrying out the action would be terrific.
	ATT3	Carrying out the action would be valuable.
	ATT4	Carrying out the action would be useful.
	ATT5	Carrying out the action would be wise
	ATT6	Carrying out the action would be attractive.
	ATT7	Carrying out the action would be pleasant.
Moral Intensity (MI)	MI1	I believe that if I undertake this action, the overall harm to others will be high.
	MI2	I believe that if I undertake this action, the likelihood of general harm to others is high.
	MI3	I believe that if I undertake this action, it would harm others in the immediate future.
	MI4	I believe that if I undertake this action, I would harm people close to me
	MI5	I believe that if I undertake this action, others would feel the negative effects very quickly.

	MI6	I believe that if I undertake this action, most people would agree that it is wrong
Intention of unethical IT use (INTENT)	INTENT1	If I were to carry out this action, it makes sense for me to do it.
	INTENT2	Depending on the situation, I could carry out this action.
	INTENT3	If I had the opportunity, I would carry out this action
	INTENT4	All things considered, it is likely that I might carry out this action in the future
	INTENT5	All things considered, I expect to carry out this action in the future
	INTENT6	I intend to carry out this action in the future.
Subjective norms (SN)	SN1	I would have the support of my fellow students if I were to carry out this action
	SN2	My fellow students would want me to carry out this action.
	SN3	My fellow students would prefer me carry out this action
	SN4	My fellow students would themselves have carried out this action if they had been in my place.
	SN5	I would have been able to take help from my friends for carrying out this action.
Perceived Behavioral Control (PBC)	PBC1	I would feel comfortable doing the act
	PBC2	If I want, I could easily carry out the act
	PBC3	I would be able to carry out the act even if there was no one to show me.
Technological Facilitation (TECHFAC)	TECHFAC1	I believe that technology enables me to carry out this action
	TECHFAC2	I believe that technology makes it easy for me to carry out this action.
	TECHFAC3	I believe that technology helps me to carry out this action.
General Computer Self Efficacy (GCSE)	GCSE1	I believe I have the ability to remove information from a computer that I no longer need
	GCSE2	I believe that I have the ability to understand common operational problems with a computer
	GCSE3	I believe that I have the ability to use a computer to display or present information in a desired manner
Non-Traceability (TRACE)	TRACE1	If I carried out this action, I believe that the computer system could not be used to detect my actions
	TRACE2	If I carried out this action, I believe it would not be possible to identify me using the computer system.
	TRACE3	If I carried out this action, I believe that the computer system could not help ascertain that I did the action.
Lack of Punishment Severity (PUNSEV)	PUNSEV1	If I were caught after committing the action, the punishment would probably not be severe.
	PUNSEV2	If I were caught after committing the action, chances are that the punishment would not be severe
	PUNSEV3	If I were caught after committing the action, the punishment would most likely not be severe

Overall Gain (OGAIN)	OGAIN1	Overall, if I committed this action, I would gain from this behavior
	OGAIN2	Overall, if I committed this action, I would benefit rather than lose from this behavior
	OGAIN3	Overall, if I committed this action, I would incur more gain than loss from this behavior
	OGAIN4	Overall, if I committed this action, I would profit significantly and suffer little damage from this behavior
Unethical IT use	BEHAVIOR	If you have acted in a similar way before, how many times have you done so? (0, 1-5, 5-10, 10-20, >20)*

Table 5-1. Items Measuring each construct
(On a Likert Scale of 1-7, ranging from "Strongly Disagree" to "Strongly Agree")

*Not on a 1-7 Likert Scale

Technological Idealism and Technological Relativism

The measures for technological idealism were adapted from the work of Forsyth and colleagues (Forsyth, 1980; Forsyth, 1981; Forsyth et al., 1988). Previous literature has identified the fact that human ethical beliefs operate along two orthogonal dimensions: idealism and relativism. The former, as discussed earlier tries to understand ethical beliefs related to the avoidance of harm on others. The latter tries to understand the ethical beliefs that go against the following of any universal sources of contact. The measures from Forsyth et al.'s work have come to be known as the Ethics Position Questionnaire and have been heavily cited and used in the areas of business ethics and remain, to this day, perhaps the most comprehensive instrument for measuring individual ethical beliefs.

In this research, since we are more concerned with the unethical use of IT, our focus was to develop a set of measures which were salient to the IS domain. With this in mind, we adapted from the works of Forsyth and colleagues where we defined the

constructs technological idealism and technological relativism. The former refers to the ethical belief that technology should not be used to harm others and the latter refers to the ethical belief that use of technology should not subscribe to a universal role of ethical conduct.

Moral Intensity

Recall that moral intensity implies the issue-related moral imperative of acting ethically in a certain situation (Jones, 1991). This means that in a case of high moral intensity, it is more imperative to act in an ethical manner as opposed to an issue of low moral intensity. For example, making personal use of office supplies has a low moral intensity than the moral intensity of changing sensitive medical information on a medical database. This research used the Moral Intensity measures from Singhapakdi et al. (1999) and Singhapakdi et al. (1996). These moral intensity measures reflected each of the six dimensions of moral intensity argued in Jones (1991) conceptualization- magnitude of consequences, social consensus, probability of effect, immediacy of effect, proximity of effect, and concentration of the effect. Each of these dimensions is reflected in one item in the instrument, thus having a total of six items.

Measures of Attitude

There is a plethora of work in IS on the TPB and hence multitude of existing studies which measures the attitude of individuals. This research adapted measures of attitude from Peace et al. (2003). The reason that the measures were adapted from this study was that this study investigated a specific type of unethical behavior- software

piracy- in the workplace. Hence the measures were deemed appropriate to be adapted from. The final measure of attitude had seven items.

Measures of Intention

Measures of Intention were adapted from Peace et al. (2003) and from Taylor and Todd (1995), together with items that were developed. The final measure of intention had six items.

Measures of Subjective Norms

Measures of subjective norms were adapted from Peace et al. (2003) and also some items were developed in order to better reflect the context of the empirical study. The final measure for subjective norms had five items.

Measures of perceived behavioral control and its antecedents

The measure of perceived behavioral control was adapted from Taylor and Todd (1995). The measures of the antecedents for each of the elements were adapted as follows. Measures of non-traceability were adapted from Pinsonneault and Heppel (1997). The measure of self-efficacy was adapted from Marakas et al.'s (2007) measure of general computer self-efficacy. Finally, the measure for technological facilitation was developed.

Measures of lack of punishment severity and benefits and overall gain

The measures for lack of punishment severity was adapted and developed from Peace et al. (2003). The measures for overall gain were developed.

Measure of unethical behavior

The measure of unethical behavior was measured by a single item objective measure which asked the students how many times they have actually acted in a similar way in the past. The student was objectively asked to respond as to how many times s/he has acted in a similar way (as described in the case scenario) before and responded on a scale of 5 (0 times, 1-5 times, 5-10 times, 10-20 times, and greater than 20 times).

Chapter 6 - Analysis and Results

This chapter presents a discussion of the analyses and results associated with this research. At first the analysis strategy is justified. Then the instrument validation is presented, followed by tests whether common method bias could be a source of concern in this study. Next the results from the evaluation of the research model hypotheses are presented.

The choice of analysis- PLS –graph

PLS-Graph (PLS), version 3.0, build 1126 was used in the analysis. PLS is a components based Structural Equation Modeling tool that enables an assessment of both the measurement model and the structural model during data analysis. In PLS, no fit statistics are generated. Rather, fit is evaluated through the examination of the regression paths and variance accounted for (R^2) in the model (Chin, 1998). While R^2 is generated automatically by the PLS-Graph program, the significance of the regression paths must be determined by examining the t-values returned during bootstrap or jackknife procedures. Based on the t-values generated during either of these respective procedures, statistical tables can then be consulted to determine the significance of the respective paths (Chin, 1998).

There are many characteristics of PLS that make it advantageous with respect to this research and these guide our choice of PLS. This is briefly discussed below.

First, compared to traditional statistical methods, PLS is advantageous as it enables simultaneous assessment of the measurement and the structural models (Fornell and Bookstein, 1982). Also, PLS does not make any distributional assumptions or

assumptions of the scale of measurement (Fornell and Bookstein, 1982). Since PLS iteratively performs factor analysis in combination with path analysis, it is also less susceptible to violations of multivariate non-normality (Thompson et al., 1995; Chin et al., 2003).

Second, using PLS has a definite advantage when any of the constructs in the model is formative. As noted by Chin (1998), an underlying assumption of covariance-based SEM techniques is that the constructs are reflective in nature. If formative constructs are used in an SEM, it leads to identification problems (Chin, 1998). While there have been attempts to work around this problem and use covariance based SEM with formative indicators, such attempts have generally been unsuccessful (MacCallum and Browne, 1993), or at the very least, are significantly more complicated than using reflective indicators for covariance based SEM (Petter et al., 2007). As recommended by a variety of researchers, (e.g. Chin at al., 1998; Barclay et al., 1995; Fornell and Bookstein 1982) using the component based PLS can resolve this problem. Additionally, in a very recent study, Petter et al. (2007) observe that PLS does not essentially differentiate between formative and reflective indicators in the fact that data analysis procedures are practically the same for both formative and reflective indicators. Since, in our model, the moral intensity construct is a formative one, it necessitates the use of PLS as the analysis of formative constructs does not necessitate any change in analysis strategy when using PLS.

Third, Partial Least Squares (PLS) can be a powerful method of analysis because it does not have rigorous demands on measurement scales, sample size, and residual distributions (Chin et al., 2003). It should be noted that PLS can work with a much

smaller sample as long as the following heuristics are followed. The heuristics are that it should be equal to the greater of the following (Chin et al., 2003)

(1) ten times the number of indicators for the scale with the largest number of formative indicators, or,

(2) ten times the largest number of structural paths directed at a particular construct in the structural model.

Fourth, PLS can be seen as an excellent technique for theory building (Fornell and Bookstein, 1982). Given that our focal concern here is the development of a theoretical understanding of unethical behavior using IT, PLS does seem to become an appropriate technique for analysis. According to Jöreskog and Wold,(1982, p 270) who note the difference between the covariance (Maximum Likelihood or ML) based models of PLS: "ML is theory-oriented, and emphasizes the transition from exploratory to confirmatory analysis. PLS is primarily intended for causal-predictive analysis in situations of high complexity but low theoretical information." Again since our focus is on developing a complex theory of unethical IT related behavior, PLS becomes a better tool for analysis. As noted by previous researchers (Chin et al., 2003), PLS is extremely suitable for both exploratory studies and confirmatory tests.

Chin et al. further substantiate this claim for the usefulness of PLS in case of theory development (2003: Appendix A, Page 5):

"Although PLS can be used for theory confirmation, it can also be used to suggest where relationships might or might not exist and to suggest propositions for later testing. As an alternative to the more widely known covariance fitting approach (exemplified by software such as LISREL, EQS, COSAN, AMOS, and SEPATH), the component-based

PLS avoids two serious problems: inadmissible solutions and factor indeterminacy (Fornell and Bookstein, 1982).

In situations where prior theory is ***strong*** [emphasis added] and further testing and development is the goal, covariance based full-information estimation methods (e.g., using Maximum Likelihood or Generalized Least Squares) are more appropriate. Yet, due to the indeterminacy of factor score estimations, there exists a loss of predictive accuracy…For application and prediction, a PLS approach is often more suitable. Under this approach, it is assumed that all the measured variance is useful variance to be explained. Since the approach estimates the latent variables as exact linear combinations of the observed measures, it avoids the indeterminacy problem and provides an exact definition of component scores."

Due to this very issue, PLS becomes a better technique to analyze complex models (Fornell et al., 1990; Fornell and Bookstein, 1982; Chin et al., 2003). As stated by Wold (1985, p. 589), "PLS comes to the fore in larger models, when the importance shifts from individual variables and parameters to packages of variables and aggregate parameters," and that in large complex models, "PLS is virtually without competition" (p. 590).

Finally, we argue that that using a PLS-based approach is also advantageous as compared to the covariance based-SEM in our case, due to the sample size. Given the total sample size of 493 (after removing missing data), a covariance based SEM would have required at least 630 subjects under normal conditions or 1260 subjects under non-normal conditions[2] (Bentler and Chou, 1988)

[2] The necessary sample size are calculated as follows: The number of parameters to be estimated for a covariance based SEM in our study, which consists of 54 indicators, is 126 (54 factor loadings + 54 error terms + 13 structural paths + 5

Manipulation Check

Recall that there were three exogenous variables that were manipulated through the case scenarios. The exogenous variables manipulated were moral intensity, Non-traceability afforded by the technology, and the lack of punishment severity as the repercussion for the act. Each of these variables was measured in the final instrument and the manipulation checks were conducted. The results for the manipulation checks are presented below.

Moral Intensity

	Group	N	Mean	Std. Deviation	Std. Error Mean
High Moral Intensity	1	267	4.1604	1.40872	.08621
Low Moral Intensity	2	226	2.7692	1.41812	.09433

Table 6-1. Group Statistics for Moral Intensity Manipulation Check

The manipulation check for moral intensity was highly successful. The score of moral intensity was computed by averaging the six items measuring moral intensity. As shown in the statistics above, there was a significant different between the means of the two sets of cases representing high and low moral intensity. The results (as shown in Tables 6-1 and 6-2) show that, true to our manipulation, the subjects rated the illegal grade change as a much higher moral intensity scenario as compared to the downloading of music.

---

endogenous error terms). Bentler and Chou (1988) provided the heuristic of 5 subjects per parameter under normal conditions or 10 subjects per parameter for non-normal conditions.

t-value	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
10.887	476.592	.000	1.3913	.12779

Table 6-2. t-Test for manipulation check of Moral Intensity

Lack of Punishment Severity

	Group	N	Mean	Std. Deviation	Std. Error Mean
Lack of Punishment Severity (LO)	1	256	2.1914	1.40441	.08778
Lack of Punishment Severity (HI)	2	237	3.7651	1.74010	.11303

Table 6-3. Group Statistics for (Lack of) Punishment Severity Manipulation Check

The manipulation check for lack of punishment severity was, again, highly successful. The score of lack of punishment severity was computed by averaging the three items measuring punishment severity (adapted from Peace et al., 2003). As shown in the statistics above, there was a significant different between the means of the two sets of cases representing high and low cases of lack of punishment severity (or, alternately, low and high cases of punishment severity). The results (as shown in Tables 6-3 and 6-4) show that, true to our manipulation, the subjects differentiated in their perceptions of punishment. For example, subjects treated a warning as a significantly low punishment (high lack of punishment severity) as compared to dismissal from the university (low lack of punishment severity).

t-value	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
-10.996	453.746	.000	-1.5737	.14311

Table 6-4. t-test for (Lack of) Punishment Severity Manipulation Check

Non-traceability

	Group	N	Mean	Std. Deviation	Std. Error Mean
Low Non-traceability	1	244	2.0792	1.23954	.07935
High non-traceability	2	249	2.9424	1.59040	.10079

Table 6-5. Group Statistics for Non-traceability Manipulation Check

Finally, the manipulation check for non-traceability was, again, highly successful. The score of non-traceability was computed by averaging the three items measuring non-traceability (adapted from Peace et al., 2003). As shown in the statistics above, there was a significant different between the means of the two sets of cases representing high and low cases of non-traceability (or, alternately, low and high cases of traceability). The results (as shown in Tables 6-5 and 6-6) show that, true to our manipulation, the subjects differentiated in their perceptions of traceability offered by technology. For example, subjects treated the existence of technological controls including audits and log files (low non-traceability) significantly differently from the non-existence of such audit and log files (high non-traceability).

t-value	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
-6.729	467.445	.000	-.8632	.12828

Table 6-6. t-test for Non-traceability Manipulation Check

Measurement model

Because many items of the instrument were adapted from past literature or were developed, particular attention was paid toward assessing the reliability and validity of the instrument prior to our hypotheses testing.

In PLS, analysis of the measurement model involves analyzing reliability, convergent validity and discriminant validity (Fornell and Larcker, 1981). A high level of composite reliability above 0.70 is recommended (Nunnally, 1978). As seen below, in Table 6-7, our composite reliabilities were much higher than the recommended threshold of 0.70, thus ensuring that our instrument was reliable.

Gefen and Straub (2005) lay down clear guidelines on assessing instrument validity using PLS. In their opinion, convergent validity "is shown when t-values of the Outer Model Loadings are above 1.96" (p. 97). Table 6-8 shows the loadings of each item on its corresponding factor and the corresponding t-value. It can be seen that the t-values for each loading are far above the recommended threshold, thereby demonstrating very high convergent validity.

Construct	Composite Reliability
Technological Idealism	0.908
Technological Relativism	0.843
Moral Intensity	0.944
Attitude	0.938
Subjective Norms	0.967
Lack of Punishment Severity	0.962
Overall Gain	0.976
Non-traceability	0.974
Self Efficacy	0.934
Technological Facilitation	0.959
Perceived Behavioral Control	0.928
Intention	0.953

Table 6-7. Composite Reliability Statistics

Variables	Loading	Standard Error	T-Statistic
IDEAL1	0.7777	0.0622	12.5092
IDEAL2	0.7069	0.1289	5.4857
IDEAL3	0.7176	0.1282	5.598
IDEAL4	0.8432	0.0421	20.0419
IDEAL5	0.8792	0.0464	18.9317
IDEAL6	0.7929	0.0616	12.8774
RELA1	0.6953	0.0749	9.2802
RELA2	0.7311	0.0591	12.3739
RELA3	0.8582	0.035	24.5421
RELA4	0.7375	0.064	11.5308
ATT1	0.9184	0.0092	100.0435
ATT2	0.8926	0.0162	55.2427
ATT3	0.7526	0.0293	25.658
ATT4	0.718	0.0273	26.3265
ATT5	0.8526	0.0141	60.3702
ATT6	0.7473	0.0277	26.9438
ATT7	0.8882	0.0106	83.83
INTENT1	0.8177	0.0188	43.5035
INTENT2	0.7372	0.0227	32.5176
INTENT3	0.9176	0.0107	85.5524
INTENT4	0.9275	0.0093	100.2681
INTENT5	0.9349	0.0065	143.2706
INTENT6	0.9186	0.0083	110.6434
MI1	0.8822	0.0162	54.4

MI2	0.8973	0.0158	56.8989
MI3	0.9118	0.0124	73.4201
MI4	0.874	0.0147	59.6358
MI5	0.8722	0.0156	55.7805
MI6	0.7045	0.0231	30.5148
SN1	0.9419	0.0103	91.0107
SN2	0.9587	0.0065	147.8804
SN3	0.9584	0.0069	139.609
SN4	0.835	0.0177	47.0797
SN5	0.918	0.0101	90.6843
PBC1	0.9269	0.0093	99.4811
PBC2	0.8433	0.0244	34.566
PBC3	0.9311	0.0106	87.7104
TRACE1	0.9564	0.0112	85.6571
TRACE2	0.9695	0.0066	147.3426
TRACE3	0.9588	0.0141	67.9831
GCSE1	0.8856	0.0134	65.9835
GCSE2	0.9292	0.0091	102.6046
GCSE3	0.9085	0.0154	58.8359
TECHFAC1	0.9253	0.0109	84.7831
TECHFAC2	0.9598	0.0082	117.1491
TECHFAC3	0.9381	0.0147	63.6768
PUNSEV1	0.9165	0.0172	53.3155
PUNSEV2	0.9506	0.01	95.1838
PUNSEV3	0.9681	0.0054	180.2739
OGAIN1	0.942	0.0097	97.0481
OGAIN2	0.9619	0.0063	151.6825
OGAIN3	0.9652	0.0062	154.9333
OGAIN4	0.9501	0.007	135.9029

Table 6-8. Factor Loadings for Convergent Validity

According to Gefen and Straub (2005), discriminant validity is assessed by a two step process: 1) the loadings of the items on their respective theoretical constructs are high while their (items') loadings on the other theoretical constructs are low and, 2) the AVE for each construct is much greater than the squared correlations between any pair of latent constructs[3]. Following Gefen and Straub's (2005) procedure of obtaining the loadings and the cross loadings for each construct (shown in Table 6-9), we can see that

[3] Alternately, the square root of the AVE is much greater than the correlations between any pair of latent constructs

the loadings of items on their respective constructs are much higher than their loadings on other constructs. Also, loadings of items on their respective constructs satisfied the usually recommended value of 0.7 (Nunnally, 1978) and exceeded it considerably in most cases. Thus, condition 1 of the discriminant validity assessment was satisfied. For condition 2, we examined the AVE for each construct and compared it to the squared correlation between any two constructs. Table 6-10 shows that the square root of the AVE for each construct is much higher than the squared correlation between any pair of latent constructs. Also, as shown in Table 6-10, all the AVE scores for each construct were higher than Fornell and Larcker's (1981) recommended value of 0.5. Thus, condition 2 for discriminant validity is also satisfied. Altogether, the measurement instrument offered acceptable psychometric properties.

	IDEAL	RELA	ATT	INTENT	MI	SN	PBC	TRACE	GCSE	TECHFAC	PUNSEV	OGAIN
IDEAL1	**0.78**	-0.09	-0.11	-0.09	0.08	-0.07	-0.02	-0.12	0.04	0.05	-0.08	-0.03
IDEAL2	**0.71**	-0.06	-0.08	-0.07	0.09	-0.08	-0.03	-0.16	-0.01	0.08	-0.05	-0.03
IDEAL3	**0.72**	-0.04	-0.05	-0.09	0.09	-0.06	-0.02	-0.10	-0.04	0.05	-0.03	-0.03
IDEAL4	**0.84**	-0.08	-0.15	-0.14	0.23	-0.07	-0.11	-0.05	-0.04	-0.07	-0.07	-0.07
IDEAL5	**0.88**	-0.11	-0.12	-0.13	0.17	-0.07	-0.11	-0.09	-0.07	-0.02	-0.07	-0.08
IDEAL6	**0.79**	-0.07	-0.11	-0.13	0.16	-0.04	-0.14	-0.10	-0.12	-0.05	-0.02	-0.08
RELA1	-0.13	**0.70**	0.18	0.18	-0.03	0.21	0.02	0.18	-0.04	0.03	0.16	0.13
RELA2	-0.04	**0.73**	0.12	0.14	0.00	0.06	0.06	0.11	0.03	-0.03	0.02	0.13
RELA3	-0.08	**0.86**	0.18	0.18	0.02	0.09	0.02	0.20	0.02	-0.07	0.06	0.19
RELA4	-0.03	**0.74**	0.12	0.13	0.06	0.09	0.02	0.17	-0.01	-0.04	0.10	0.11
ATT1	-0.17	0.22	**0.92**	0.67	-0.40	0.55	0.25	0.38	0.06	0.16	0.41	0.61
ATT2	-0.12	0.26	**0.89**	0.65	-0.35	0.50	0.22	0.38	0.06	0.12	0.39	0.55
ATT3	-0.09	0.14	**0.75**	0.45	-0.29	0.39	0.18	0.22	0.10	0.21	0.28	0.55
ATT4	-0.06	0.07	**0.72**	0.41	-0.30	0.42	0.18	0.20	0.06	0.23	0.28	0.50
ATT5	-0.17	0.23	**0.85**	0.62	-0.33	0.53	0.21	0.47	0.06	0.08	0.46	0.56
ATT6	-0.06	0.02	**0.75**	0.45	-0.28	0.41	0.22	0.25	0.08	0.14	0.35	0.48
ATT7	-0.10	0.18	**0.89**	0.65	-0.41	0.60	0.28	0.37	0.13	0.19	0.48	0.59
INTENT1	-0.11	0.21	0.60	**0.82**	-0.45	0.54	0.56	0.40	0.20	0.31	0.39	0.60
INTENT2	-0.13	0.08	0.45	**0.74**	-0.40	0.46	0.65	0.20	0.34	0.44	0.31	0.46

INTENT3	-0.12	0.22	0.67	**0.92**	-0.46	0.58	0.43	0.41	0.14	0.27	0.38	0.58
INTENT4	-0.14	0.19	0.66	**0.93**	-0.43	0.63	0.40	0.40	0.13	0.32	0.43	0.53
INTENT5	-0.13	0.21	0.63	**0.93**	-0.41	0.62	0.41	0.40	0.12	0.29	0.43	0.50
INTENT6	-0.13	0.20	0.61	**0.92**	-0.39	0.61	0.39	0.41	0.13	0.29	0.42	0.48
MI1	0.17	0.05	-0.29	-0.34	**0.88**	-0.34	-0.28	-0.09	-0.18	-0.24	-0.11	-0.33
MI2	0.17	0.05	-0.28	-0.34	**0.90**	-0.34	-0.26	-0.07	-0.18	-0.22	-0.09	-0.31
MI3	0.15	0.03	-0.31	-0.37	**0.91**	-0.37	-0.29	-0.10	-0.16	-0.22	-0.15	-0.32
MI4	0.12	0.05	-0.34	-0.39	**0.87**	-0.42	-0.34	-0.14	-0.16	-0.33	-0.24	-0.38
MI5	0.15	0.05	-0.33	-0.37	**0.87**	-0.43	-0.29	-0.15	-0.17	-0.26	-0.23	-0.38
MI6	0.18	-0.11	-0.47	-0.54	**0.70**	-0.65	-0.26	-0.27	-0.10	-0.26	-0.40	-0.35
SN1	-0.09	0.20	0.55	0.63	-0.49	**0.94**	0.32	0.35	0.09	0.30	0.41	0.44
SN2	-0.06	0.18	0.55	0.62	-0.51	**0.96**	0.33	0.33	0.10	0.30	0.41	0.44
SN3	-0.07	0.18	0.55	0.62	-0.49	**0.96**	0.33	0.35	0.09	0.29	0.41	0.43
SN4	-0.06	0.06	0.57	0.53	-0.47	**0.84**	0.28	0.31	0.09	0.30	0.36	0.46
SN5	-0.09	0.12	0.54	0.61	-0.48	**0.92**	0.32	0.35	0.12	0.30	0.39	0.44
PBC1	-0.11	0.05	0.30	0.53	-0.35	0.35	**0.93**	0.15	0.43	0.47	0.25	0.36
PBC2	-0.05	0.02	0.17	0.40	-0.23	0.26	**0.84**	0.11	0.41	0.38	0.15	0.23
PBC3	-0.11	0.04	0.24	0.49	-0.33	0.31	**0.93**	0.09	0.48	0.52	0.20	0.28
TRACE1	-0.12	0.23	0.40	0.43	-0.18	0.36	0.13	**0.96**	0.02	0.03	0.34	0.42
TRACE2	-0.13	0.21	0.39	0.42	-0.18	0.36	0.13	**0.97**	0.01	0.05	0.33	0.41
TRACE3	-0.10	0.21	0.38	0.38	-0.15	0.34	0.11	**0.96**	0.00	0.05	0.32	0.38
GCSE1	-0.06	0.00	0.14	0.23	-0.18	0.12	0.48	0.05	**0.89**	0.35	0.09	0.21
GCSE2	-0.04	0.02	0.07	0.17	-0.15	0.08	0.44	0.01	**0.93**	0.33	0.04	0.13
GCSE3	-0.04	-0.04	0.04	0.11	-0.16	0.08	0.41	-0.04	**0.91**	0.35	-0.02	0.10
TECHFAC1	-0.03	-0.06	0.16	0.31	-0.27	0.30	0.48	0.04	0.34	**0.93**	0.18	0.21
TECHFAC2	-0.01	-0.01	0.19	0.37	-0.28	0.32	0.51	0.06	0.37	**0.96**	0.24	0.22
TECHFAC3	0.01	-0.04	0.18	0.34	-0.31	0.29	0.46	0.03	0.35	**0.94**	0.24	0.26
PUNSEV1	-0.08	0.10	0.43	0.43	-0.26	0.40	0.23	0.29	0.05	0.22	**0.92**	0.42
PUNSEV2	-0.05	0.10	0.44	0.41	-0.23	0.40	0.19	0.32	0.03	0.22	**0.95**	0.43
PUNSEV3	-0.06	0.14	0.45	0.44	-0.25	0.43	0.23	0.36	0.05	0.22	**0.97**	0.44
OGAIN1	-0.07	0.17	0.62	0.56	-0.40	0.47	0.32	0.38	0.18	0.25	0.41	**0.94**
OGAIN2	-0.07	0.17	0.64	0.60	-0.41	0.48	0.32	0.41	0.19	0.25	0.44	**0.96**
OGAIN3	-0.07	0.20	0.64	0.57	-0.40	0.44	0.31	0.39	0.15	0.23	0.44	**0.97**
OGAIN4	-0.06	0.19	0.63	0.55	-0.35	0.43	0.29	0.41	0.13	0.20	0.45	**0.95**

Table 6-9. Factor Loadings and Cross Loadings for Discriminant Validity

	IDEAL	RELA	ATT	INTENT	MI	SN	BEHAVIOR	PBC	TRACE	GCSE	TECHFAC	PUNSEV	OGAIN
IDEAL	**0.79**												
RELA	-0.10	**0.76**											
ATT	-0.14	0.21	**0.83**										
INTENT	-0.14	0.22	0.69	**0.88**									
MI	0.19	0.01	-0.41	-0.48	**0.86**								
SN	-0.08	0.16	0.60	0.65	-0.53	**0.92**							
BEHAVIOR	-0.05	0.13	0.40	0.67	-0.44	0.55	**1.00**						
PBC	-0.10	0.04	0.27	0.53	-0.34	0.34	0.35	**0.9**					
TRACE	-0.12	0.23	0.41	0.43	-0.18	0.37	0.17	0.13	**0.96**				
GCSE	-0.05	0.00	0.09	0.19	-0.18	0.11	0.15	0.49	0.01	**0.91**			
TECHFAC	-0.01	-0.04	0.19	0.36	-0.30	0.32	0.35	0.51	0.05	0.38	**0.94**		
PUNSEV	-0.07	0.12	0.47	0.45	-0.26	0.43	0.26	0.23	0.34	0.05	0.23	**0.94**	
OGAIN	-0.07	0.19	0.67	0.60	-0.41	0.48	0.32	0.33	0.42	0.17	0.24	0.46	**0.95**

Ascertaining existence of common method bias

Any empirical study conducted has possibilities of common methods bias. Podsakoff et al. (2003) define common methods bias as the existence of variance that is attributable to the measurement method (i.e. in the way the empirical study has been conducted rather than due to the constructs themselves). As noted by Podsakoff et al. (2003), they are a problem as they constitute a major source of measurement error, which threatens the validity of the conclusions between the measure. According to Bagozzi and Yi (1991), such method biases can arise from a variety of sources:

Method variance refers to variance that is attributable to the measurement method rather than to the construct of interest. The term method refers to the form of measurement at different levels of abstraction, such as the content of specific items, scale type, response format, and the general context (Fiske, 1982, pp. 81–84). At a more abstract level,

method effects might be interpreted in terms of response biases such as halo effects, social desirability, acquiescence, leniency effects, or yea- and nay-saying. (p. 426)

Such common method biases have both a random component and a systematic component (Bagozzi & Yi, 1991; Nunnally, 1978; Spector, 1987; Podsakoff et al., 2003). Of special concern in occurrences of such common method biases is the systematic error variance which can have serious confounding implications on the results of an empirical study, including misleading conclusions (Campbell and Fiske, 1959; Podsakoff et al., 2003).

Given this scenario, there is a need to detect if there is any occurrence of common methods biases in this research. The procedure to detect such common method biases closely followed Pavlou et al.'s (2007) recommended steps. We describe each of the tests below.

Harman's Single factor Test

This test is perhaps the most widely used test for detecting common method biases (Podsakoff et al., 2003).

This test involves the simultaneous loading of all constructs into an exploratory factor analysis (Andersson and Bateman, 1997; Aulakh and Gencturk, 2000; Greene and Organ, 1973; Organ and Greene, 1981; Schriesheim, 1979) and examining the unrotated factor solutions to determine the number of factors that become necessary to explain the variance observed in the constructs (Podsakoff et al., 2003). As Podsakoff et al. (2003) note, the basic underlying assumption of this test is that if there is a common methods bias, then there shall be a significant amount of common method variance explained by a

single factor and subsequently, it will explain the majority of the covariance between the constructs.

		Initial Eigenvalues			Extraction Sums of Squared Loadings		Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	16.80	31.71	31.71	16.80	31.71	31.71	4.79	9.04	9.04
2	4.82	9.09	40.80	4.82	9.09	40.80	4.68	8.83	17.88
3	3.87	7.31	48.10	3.87	7.31	48.10	4.40	8.30	26.18
4	3.20	6.05	54.15	3.20	6.05	54.15	4.31	8.13	34.31
5	2.49	4.69	58.84	2.49	4.69	58.84	3.87	7.29	41.60
6	2.21	4.18	63.02	2.21	4.18	63.02	3.40	6.42	48.03
7	1.99	3.76	66.78	1.99	3.76	66.78	3.18	6.00	54.03
8	1.76	3.31	70.09	1.76	3.31	70.09	2.96	5.58	59.61
9	1.53	2.89	72.98	1.53	2.89	72.98	2.92	5.51	65.13
10	1.46	2.76	75.75	1.46	2.76	75.75	2.78	5.25	70.37
11	1.22	2.31	78.06	1.22	2.31	78.06	2.58	4.87	75.24
12	1.01	1.92	79.97	1.01	1.92	79.97	2.51	4.73	79.97
13	0.89	1.67	81.64						
14	0.83	1.56	83.20						
15	0.71	1.35	84.55						
16	0.63	1.19	85.74						
17	0.52	0.99	86.72						
18	0.49	0.93	87.65						
19	0.47	0.88	88.53						
20	0.44	0.82	89.35						
21	0.38	0.71	90.07						
22	0.36	0.69	90.75						
23	0.36	0.67	91.42						
24	0.35	0.65	92.08						
25	0.31	0.59	92.67						
26	0.29	0.55	93.22						
27	0.25	0.48	93.69						
28	0.25	0.47	94.17						
29	0.24	0.45	94.61						
30	0.22	0.42	95.04						
31	0.20	0.38	95.42						
32	0.19	0.37	95.79						

33	0.19	0.36	96.15						
34	0.18	0.35	96.49						
35	0.18	0.33	96.83						
36	0.16	0.30	97.13						
37	0.15	0.29	97.41						
38	0.15	0.28	97.69						
39	0.14	0.27	97.96						
40	0.13	0.24	98.20						
41	0.11	0.21	98.41						
42	0.11	0.20	98.61						
43	0.11	0.20	98.81						
44	0.10	0.18	98.99						
45	0.09	0.17	99.16						
46	0.08	0.16	99.32						
47	0.08	0.14	99.46						
48	0.07	0.13	99.59						
49	0.06	0.11	99.70						
50	0.06	0.10	99.80						
51	0.05	0.09	99.90						
52	0.03	0.05	99.95						
53	0.03	0.05	100.00						

Table 6-11. Total variance Explained (test for common methods bias)

Variables	**Component**											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
IDEAL1	-0.13	-0.14	0.73	-0.16	0.06	0.15	-0.07	-0.03	-0.02	-0.04	0.05	-0.04
IDEAL2	-0.12	-0.13	0.74	-0.16	0.10	0.13	0.04	0.08	-0.09	0.05	0.18	0.09
IDEAL3	-0.11	-0.08	0.76	-0.18	0.08	0.14	-0.01	0.07	-0.09	0.05	0.20	0.16
IDEAL4	-0.19	0.06	0.75	-0.08	-0.04	0.12	-0.13	-0.14	0.05	-0.12	-0.12	-0.09
IDEAL5	-0.18	0.00	0.80	-0.18	-0.02	0.13	-0.08	-0.09	0.01	-0.05	-0.01	-0.04
IDEAL6	-0.17	0.06	0.71	-0.19	-0.08	0.08	-0.08	-0.02	0.00	-0.10	-0.10	-0.01
RELA1	0.21	0.26	-0.08	0.19	-0.11	0.30	0.09	0.32	0.12	0.06	0.00	0.12
RELA2	0.13	0.20	-0.01	0.27	0.15	0.59	0.13	0.35	0.04	0.01	0.04	0.01
RELA3	0.18	0.32	-0.05	0.32	0.16	0.60	0.10	0.35	0.06	0.01	0.04	0.02
RELA4	0.13	0.29	0.00	0.31	0.04	0.53	0.06	0.38	0.06	-0.02	0.03	0.04
MI1	-0.49	0.42	0.25	0.53	-0.17	-0.21	0.15	-0.06	0.06	0.01	-0.09	-0.02
MI2	-0.48	0.41	0.26	0.56	-0.16	-0.23	0.14	-0.07	0.06	0.03	-0.10	0.00
MI3	-0.52	0.39	0.24	0.55	-0.12	-0.23	0.16	-0.07	0.09	0.06	-0.09	-0.02
MI4	-0.56	0.38	0.15	0.47	-0.07	-0.10	0.18	-0.14	0.05	-0.01	-0.04	-0.04
MI5	-0.55	0.34	0.19	0.49	-0.06	-0.12	0.19	-0.09	-0.01	0.06	-0.03	0.02
MI6	-0.65	0.04	0.13	0.24	0.30	-0.08	0.01	-0.07	-0.05	0.12	-0.08	0.09

ATT1	0.77	0.28	-0.01	-0.04	0.15	-0.05	0.25	-0.10	-0.04	-0.06	0.18	0.01
ATT2	0.73	0.30	0.04	-0.02	0.16	0.01	0.24	-0.11	-0.07	-0.08	0.24	0.02
ATT3	0.59	0.13	0.07	-0.07	0.35	-0.16	0.33	-0.01	0.20	0.16	0.13	0.16
ATT4	0.57	0.09	0.10	-0.14	0.29	-0.21	0.32	-0.02	0.24	0.19	0.13	0.22
ATT5	0.72	0.36	-0.02	0.02	0.09	-0.06	0.11	-0.12	0.01	-0.13	0.18	0.01
ATT6	0.59	0.16	0.10	-0.09	0.21	-0.27	0.23	-0.13	0.09	-0.03	0.15	0.23
ATT7	0.78	0.22	0.07	-0.06	0.10	-0.10	0.20	-0.07	0.05	-0.13	0.19	0.04
PUNSEV1	0.55	0.16	0.10	0.08	-0.14	-0.39	-0.21	0.42	-0.13	-0.28	0.06	0.08
PUNSEV2	0.54	0.21	0.13	0.08	-0.15	-0.41	-0.24	0.44	-0.10	-0.28	0.09	0.02
PUNSEV3	0.57	0.21	0.12	0.10	-0.16	-0.36	-0.26	0.44	-0.09	-0.29	0.09	0.05
OGAIN1	0.73	0.10	0.11	-0.01	0.41	-0.08	-0.09	0.07	0.10	0.09	-0.32	-0.14
OGAIN2	0.76	0.11	0.11	0.01	0.40	-0.09	-0.11	0.06	0.07	0.07	-0.30	-0.19
OGAIN3	0.74	0.13	0.11	-0.01	0.44	-0.09	-0.10	0.11	0.03	0.07	-0.30	-0.15
OGAIN4	0.71	0.17	0.12	0.02	0.43	-0.12	-0.11	0.09	0.04	0.07	-0.33	-0.13
SN1	0.75	0.06	0.05	-0.12	-0.45	0.12	0.10	-0.02	0.24	-0.03	-0.15	0.01
SN2	0.75	0.04	0.07	-0.15	-0.44	0.11	0.10	-0.03	0.25	-0.05	-0.17	0.02
SN3	0.75	0.06	0.06	-0.13	-0.46	0.11	0.09	-0.04	0.25	-0.05	-0.17	0.04
SN4	0.70	0.02	0.08	-0.20	-0.25	-0.03	0.11	-0.07	0.30	0.06	-0.11	0.13
SN5	0.74	0.03	0.05	-0.12	-0.40	0.05	0.08	-0.08	0.27	-0.03	-0.16	0.03
TRACE1	0.51	0.41	-0.04	0.17	-0.02	0.11	-0.57	-0.24	0.07	0.17	0.14	0.08
TRACE2	0.50	0.40	-0.04	0.17	-0.04	0.09	-0.58	-0.25	0.08	0.21	0.15	0.10
TRACE3	0.47	0.40	-0.02	0.18	-0.04	0.09	-0.59	-0.24	0.10	0.22	0.18	0.11
GCSE1	0.29	-0.50	0.03	0.40	0.19	0.02	-0.08	-0.14	0.25	-0.32	0.12	-0.12
GCSE2	0.22	-0.54	0.03	0.42	0.18	0.09	-0.07	-0.14	0.31	-0.38	0.16	-0.14
GCSE3	0.18	-0.59	0.02	0.36	0.18	0.07	-0.06	-0.15	0.38	-0.31	0.14	-0.12
PBC1	0.55	-0.47	0.04	0.33	0.01	0.03	-0.01	-0.06	-0.22	-0.04	-0.19	0.31
PBC2	0.40	-0.45	0.05	0.35	-0.04	0.07	-0.05	-0.14	-0.19	-0.08	-0.21	0.31
PBC3	0.50	-0.55	0.04	0.35	-0.01	0.04	0.02	-0.04	-0.21	-0.02	-0.11	0.33
INTENT1	0.78	-0.04	0.05	0.12	0.08	0.11	0.01	-0.09	-0.26	0.04	-0.12	0.13
INTENT2	0.67	-0.30	0.03	0.20	0.00	0.01	0.09	-0.08	-0.26	0.01	-0.15	0.09
INTENT3	0.81	0.07	0.04	0.06	-0.01	0.13	0.12	-0.16	-0.30	0.02	0.02	-0.12
INTENT5	0.81	0.09	0.03	0.08	-0.15	0.07	0.15	-0.14	-0.28	0.00	0.08	-0.25
INTENT6	0.79	0.11	0.04	0.11	-0.19	0.09	0.14	-0.15	-0.32	-0.02	0.08	-0.26
INTENT7	0.77	0.11	0.03	0.11	-0.20	0.10	0.11	-0.17	-0.30	-0.02	0.09	-0.29
TECHFAC1	0.39	-0.54	0.14	0.22	-0.19	-0.18	0.03	0.18	0.10	0.44	0.12	-0.12
TECHFAC2	0.43	-0.55	0.17	0.26	-0.18	-0.14	0.02	0.21	0.07	0.42	0.18	-0.12
TECHFAC3	0.41	-0.55	0.18	0.18	-0.13	-0.17	0.00	0.25	0.05	0.41	0.14	-0.17

Table 6-12. Un-rotated Component Matrix (test for common methods bias)

As noted in Tables 6-11 and 6-12 above, there were 12 components extracted from the exploratory factor analysis. This matched with the total number of constructs (12) in our study. There were 12 factors that explained the overall variance in the EFA and also the items loaded on 12 factors. This shows that our empirical measures pass the Harman's one factor test.

Lindell and Whitney Test

Next we applied the Lindell and Whitney's (2001) test as noted in Pavlou et al. (2007). In this test, a theoretically unrelated variable is added to the PLS model and its correlations with the principal endogenous constructs evaluated. In this case, we used the variable that captured the sequence in which the respondents completed the study (intRespKey). As noted by Pavlou et al. (2007), if there is a high correlation between any of the study's major constructs and this variable, it would indicate the possible existence of common method biases as the variable intRespKey should be weakly related to any construct in the study. Our results show that indeed, there is a very weak correlation between this variable and the other constructs in the study. This shows that common methods bias is not a major concern.

Correlation between the latent variables

Finally, as noted by Pavlou et al. (2007), the correlation matrix (as shown in the section on the measurement model) does not indicate that any of the factors are highly correlated with one. The highest correlation noted was 0.69; however in case of common method biases, there should have existed extremely high correlations of the order of 0.90

(Pavlou et al., 2007). All these tests together show that existence of common method biases is not a major concern in this study.

Structural Model

Having demonstrated acceptable psychometric properties for our measurement instrument, we proceed to test the structural model. Figure 6-1 shows the structural model.

In PLS, the predictive power of the structural model can be known by the variance explained in the endogenous constructs (Chin, 1998; Petter et al., 2007). Falk and Miller (1992) mention that a substantive model should explain at least 10% of the variance in endogenous constructs. With this benchmark, our model shows substantial predictive power. As shown in the Figure 6-1 below, 21.7% of the variance in attitude toward unethical IT use, 20.7% of variance in overall gain, 66.2% of the variance in intention to use IT unethically, 38% in the variance in perceived behavioral control, and 44.6% of the variance in actual unethical use of IT is explained by the structural model. Observing that the model has substantive predictive power, we now turned our attention to the path coefficients for the model and the hypothesis testing. The hypothesis testing is presented in Table 6-14.

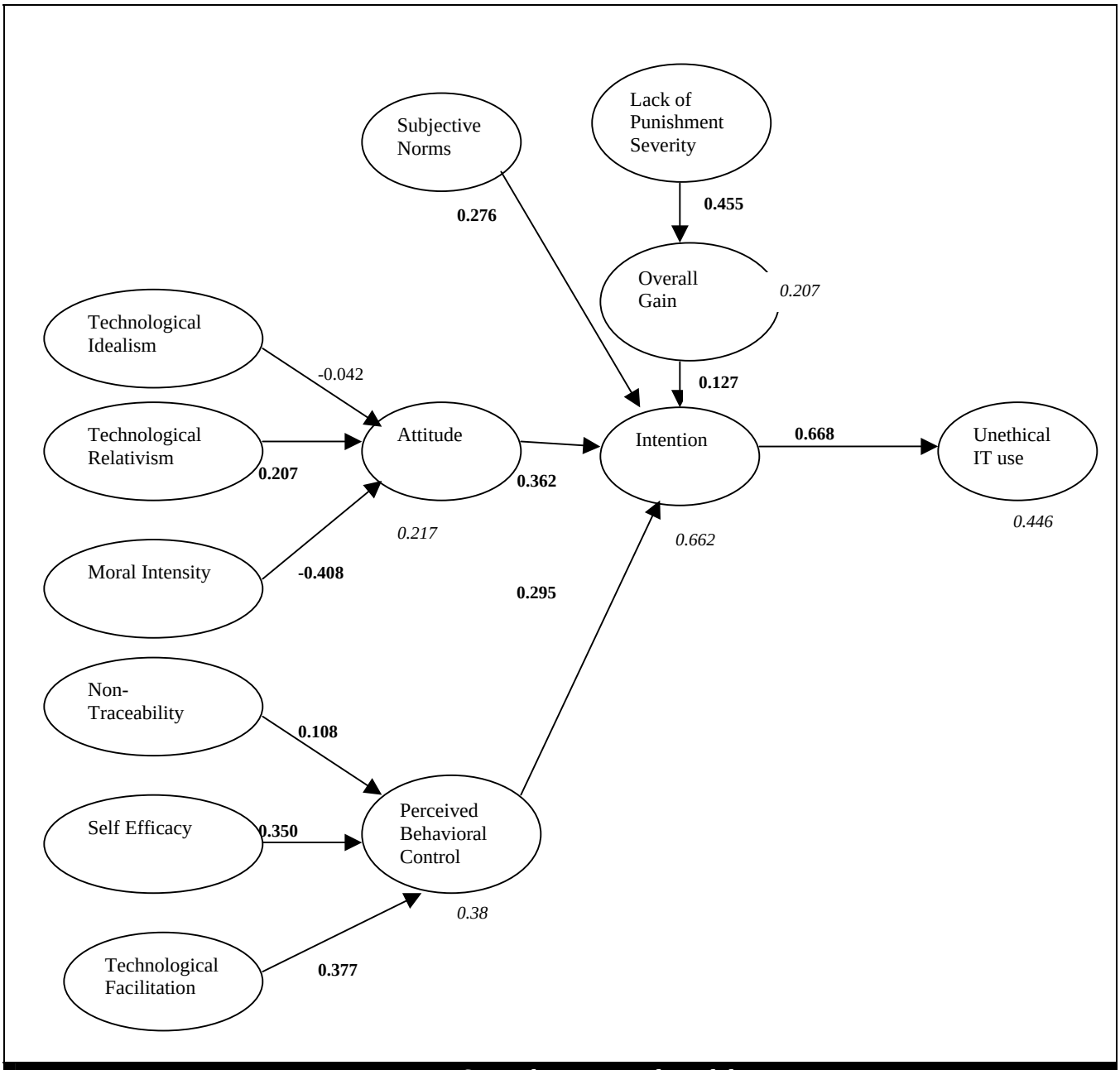

Figure 6-1. The structural model

(Significant path coefficients are noted in bold and the variances in the endogenous constructs are noted in italics)

Hypotheses number	Causal Direction	Significance	Supported
H1	Attitude->Intention (+)	p<0.001	Yes
H2	Technological Idealism->Attitude (-)	Non-significant	No
H3	Technological Relativism ->Attitude (+)	p<0.001	Yes
H4	Moral Intensity-> Attitude (-)	p<0.001	Yes
H5	Lack of Punishment Severity ->Overall Gain (+)	p<0.001	Yes
H6	Overall Gain->Intention (+)	p<0.01	Yes
H7	Subjective Norms->Intention (+)	p<0.001	Yes
H8	Perceived Behavioral Control->Intention (+)	p<0.001	Yes
H9	Non-traceability->Perceived Behavioral Control (+)	p<0.001	Yes
H10	Technological facilitation->Perceived Behavioral Control (+)	p<0.001	Yes
H11	Self efficacy-> Perceived Behavioral Control (+)	p<0.001	Yes
H12	Intention->Unethical IT use (+)	p<0.001	Yes

Table 6-14. Results of Hypotheses Testing

As indicated above, our results provide general support for all our hypotheses with the exception of the effect of technological idealism on attitude toward unethical IT use. Other than that, we found, as per our expectations, that ethical beliefs about technology (technological relativism) and the act (moral intensity) both strongly influence attitude toward unethical IT use. Attitude toward unethical IT use, subjective norms, perceived behavioral control, and overall gain perceived from committing the act, all strongly influence intentions of unethical IT use. Furthermore, overall perceptions of gain were strongly influenced by the perceptions of punishment of the act. Intentions of unethical IT use strongly influences actual behavior of unethical IT use and perceived behavioral control is strongly predicted by the technological facilitation of the unethical

act, the general computer self efficacy of the individual, and the lack of traceability provided by the technology. Our results are tabulated above.

The effect sizes for each of the predictor variables on the outcome variable were also calculated. As recommended by Chin et al. (1998), the effect size (f^2) of one variable on another is determined as follows:

$f^2 =$ *((R^2 with predictor included)- (R^2 with predictor excluded))/(1- R^2 with predictor included)*

The effect sizes for each of the predictor variables are mentioned in Table 6-13. In order to calculate the effect size of each of the predictor variables, one variable was removed at a time and the corresponding difference in variance noted when it was re-introduced back into the model.

Causal Effect	Effect Size	Effect Size Interpretation
Technological Idealism->Attitude	0.002	-
Technological Relativism->Attitude	0.04	Small Effect Size
Moral Intensity-> Attitude	0.20	Medium Effect Size
Attitude->Intention	0.17	Medium Effect Size
Subjective Norms->Intention	0.13	Medium Effect Size
Overall Gain->Intention	0.03	Small Effect Size
Lack of Punishment Severity->Overall Gain	0.207	Medium Effect Size
Perceived Behavioral Control->Intention	0.22	Medium Effect Size
Intention->Unethical IT use	0.58	Large Effect Size
Non-traceability->Perceived Behavioral Control	0.02	Small Effect Size
Self efficacy->	0.17	Medium Effect Size

Perceived Behavioral Control		
Technological facilitation->Perceived Behavioral Control	0.2	Medium Effect Size

Table 6-15. Effect Sizes

As recommended by Chin et al. (2003), drawing upon Cohen (1988), effect sizes of 0.02, 0.15 and 0.35 are interpreted as small, medium, and large respectively. Given this heuristic, we find that many of the relationships posited in the study are have medium effect sizes. While some of the other effect sizes are small, we should not forget that a small effect size need not be insignificant and can easily assume importance (Chin et al., 2003). In fact, as can be seen in the structural model and in Table 6-13, most of the path coefficients corresponding effect sizes are highly significant, at the $p<0.001$ level.

Alternate Models

Specifying alternate models are an important part of any path analysis endeavor and indeed, they have received justification in prior research. Since in this research we are building new theory using the TPB framework, it remains to be seen whether there are any other alternate models that can explain unethical use of IT. Specifying alternate models has been recommended in prior literature. As Hulland (1999) notes:
"There is nothing inherently wrong in making use of alternative models. Indeed, in the early stages of theory refinement such comparisons often play a critical role" (p. 196). Given that a core focus of this research is to develop a good theory about unethical behavior, specifying alternate models is seen as a fruitful and important endeavor.

However, if we are use specify different conceptual models, there should be a rationale on which these models are specified. Herein we discuss the alternate models

that were specified and the rationale for each. We also discuss the results of each alternate model specification.

The first alternate model that we specify is that of the theory of reasoned action (TRA). The main difference between the TPB and the TRA is that the TRA does not factor in the perceived behavioral control that is deemed as an important factor in the TPB. The TRA was proposed by Fishbein and Ajzen (1975) and continues to be an important framework to understand human behavior. The robustness of the TRA in predicting behavior has been empirically verified. Sheppard et al. (1988) conducted a meta analysis of the TRA and showed that it held across a wide range of behaviors and contexts. Naturally, given the robustness of the TRA, it gives us an alternate model (though not different from the TPB) in order to understand human behavior.

The alternately specified model based on the TRA is presented in Figure 6-2. As can be noted, there is a significant difference in the variance of intention of unethical use of IT when we use the TRA. Thus, TRA seems to be a poorer predictor of this phenomenon than TPB. In TRA, the difference in variance explained in intention to commit unethical behavior is significantly lower. As can be seen using TRA, the variance explained in intention to use IT unethically is 58.8% as compared to TPB that explains 66.2% variance in intention to use IT unethically. This shows that TPB is of greater value in predicting unethical behavior, especially since it factors in an important variable in terms of the perceived behavioral control that is a strong predictor of intention.

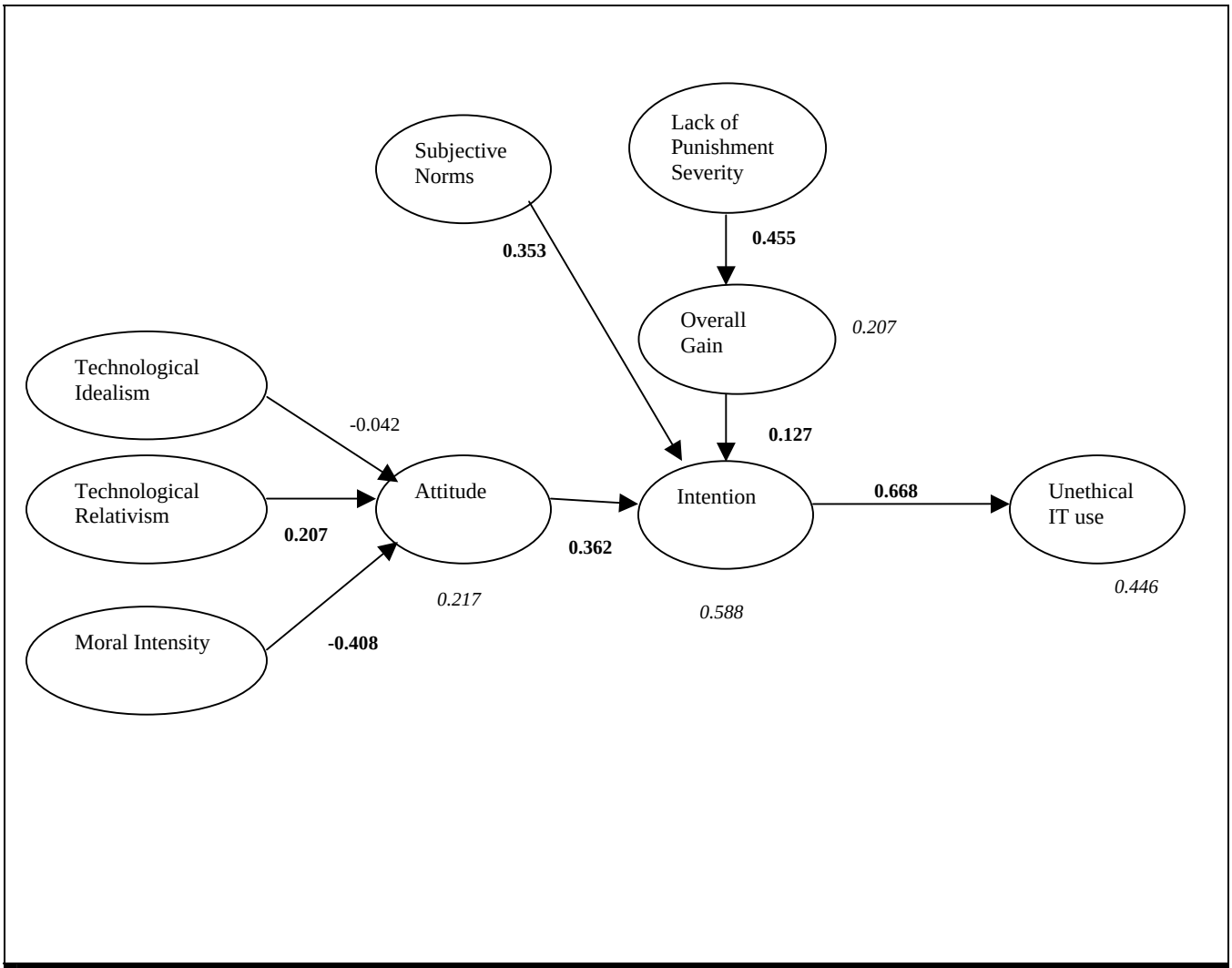

Figure 6-2. Alternate Model-the Theory of Reasoned Action

(Significant paths and variance in endogenous constructs noted as in Figure 6-1)

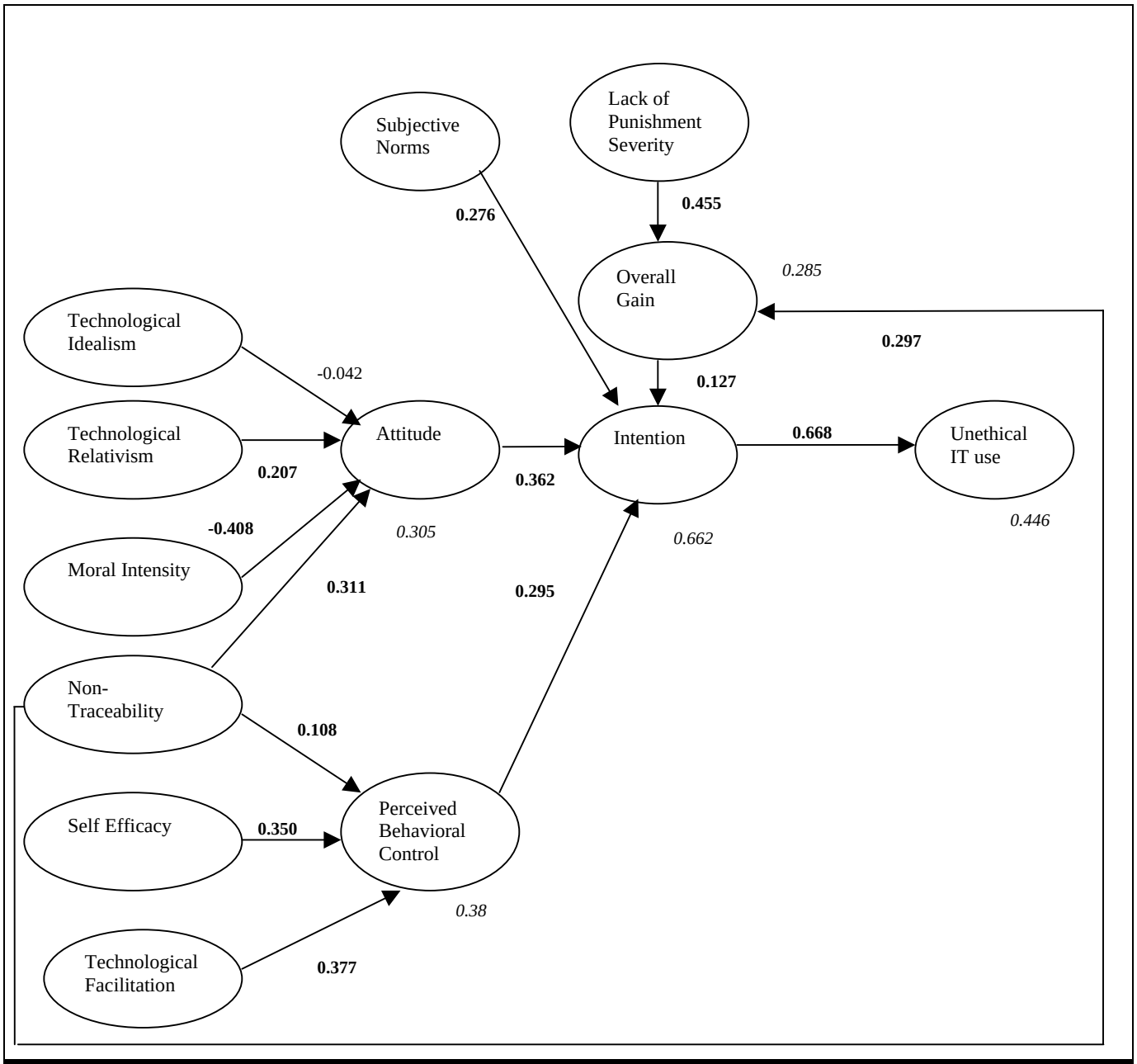

Figure 6-3. Alternate Model: non-traceability influencing overall gain and attitude (Significant paths and variance in endogenous constructs noted as in Figure 6-1)

The second alternate model specified was based on the TPB. However, this alternate model added two paths from the non-traceability of technology to attitude toward unethical IT use and overall gain respectively. There was a rationale behind adding these extra paths to the existing model. The first one was that while non-

traceability can be theoretically argued to be a predictor of perceived behavioral control, it can also be argued to be an important factor in the individual's cost benefit analysis of committing an unethical act. This is because the non-traceability offered by technology could possibly make one feel that there is a very low likelihood of getting caught upon committing an unethical act. Hence the overall perception of gain is increased because the possibility of costs (sanctions) is reduced.

The second reason is that while ethical beliefs regarding the use of technology is a theoretically important predictor of attitude toward unethical use of technology, the beliefs regarding the control that technology offers is also a possible factor in developing attitude toward unethical IT use. In other words, while attitudes toward unethical IT use definitely have an ethical component, they definitely can also be argued to have a rational component.

The structural model for this alternate specification shows a good degree of convergence with the additional conceptualization presented above. Non-traceability offered by technology significantly increases the variance explained in the attitude toward unethical IT use. While our initial model explained about 21.7% of the variance in attitude, this new model specified explains about 30.5% variance in the attitude. In addition, the path coefficient (0.311) is also highly significant ($p<0.001$).

Similarly, the addition of the path from non-traceability to overall gain significantly increases the variance in the perceptions of overall gain in committing the unethical act. While the variance explained in overall gain was previously 20.7%, it increases to 28.5% upon the addition of this new path. Additionally, the path coefficient (0.297) is also highly significant ($p<0.001$).

The alternate specifications of the model presented in this research point out that technological components are an especially important factor in understanding unethical IT use (of course in mediated by other variables). While technological considerations have already been proved (in the original model) to be important considerations for unethical behavior, the alternate model specification (the second specification) shows that it is perhaps even more important than previously hypothesized.

Chapter 7 - Discussion and Limitations

Discussion

The empirical results have important implications. The findings provide insights on why individuals use IT unethically, a key concern in today's IT enabled world. It seems that the one of the most important factors in such unethical IT use is the actual moral intensity of the act, the effect of which significantly surpasses the effect of personal beliefs related to use of IT, in the form of technological idealism and relativism. Indeed, our results show that respondents favored the illegal downloading of music scenario more than the scenario related to hacking into the computer. This is not surprising, but it reinforces the fact that individual ethical decision-making is essentially a relativistic process.

There is no surprise in the fact that attitude toward unethical IT use turned out to be a strong predictor of intentions toward unethical IT use. What is an interesting result, however, is the fact that behavioral control was (almost) as much a strong predictor of intentions as attitude was, while subjective norms was a lesser predictor than both. This point implies that, in effect, unethical use of IT definitely has a more individualistic note to it, where subjective norms have less precedence than individual beliefs and perceptions of ability. This is consistent with the fact that interactions with technology definitely draw us away from social settings and cause reduced social presence (Chatterjee, 2007), leading to the suspension of our common social beliefs and actions. In other words, when we interact with IT, we are not really in a social scenario and thus subjective norms assume much less importance.

The fact that lack of punishment severity is still a strong predictor of overall gain and that overall gain is a strong predictor of intention, points to the fundamental assumptions of many economists, particularly of the TCE stream, that human beings are by nature opportunistic and may be inclined to carry out an unethical act if there is no retribution. The fact that this lack of punishment severity significantly increases one's perceptions of gains from an unethical act (which ultimately significantly influences intention), highlights the need for strict, elaborate, and enforceable laws/policies in order to curb these actions. An important implication of this finding is that fear of punishment is an important deterrent for unethically using IT. This result proves that, to a large extent it is the fear of punishment that keeps us away from unethically using IT and hence stricter laws and policies regarding unethical use of IT are needed so as to increase this perception of punishment.

The importance of perceived behavioral control and the fact that it has a strong effect on intention of unethical IT use is interesting. Moreover, perceived behavioral control is strongly predicted by the individual's perceptions about ability to use and manipulate IT, and this has deep ramifications. While we inherently want to move toward a world of greater computer literacy and expertise, we should acknowledge that this comes at a price. Greater proficiency in IT not only leads to benefits, but it also results in more unethical use of IT. In this context, we observe that if we are to reap the benefits of the information age without experiencing negative effects of unethical IT use, we should focus on the developing greater moral instincts among IT users and develop social and technological preventive measures.

Next, the importance of technology (specifically traceability) as a strong predictor of perceived behavioral control in order to carry out an unethical act has interesting ramifications for investigating the nature of technology. What this implies is that technological controls need to be designed better and that surveillance of IT use need to be promoted. This need creates an inherent tension in the fact that surveillance by itself has ethical implications (as it violates one's right to privacy), while an absence of surveillance and monitoring creates opportunities for unethical IT use. Administrators and policy makers need to keep this issue in mind and strike a fine balance. Also, designers need to take up the issue of infusing greater controls as an inherent part of the technology. In effect we raise a call for greater auditability of technology use. We also call for systematic development of roles and functions in order to enable such audits. Also, technology applications should be designed in such a way so as to capture "footprints" of any action using that system. However, one can argue that the development and implementation of such technological and social controls may not necessarily be enough to stop such unethical use. This is because, as per our other empirical result, technology itself makes it easy to act unethically. Also, IT can always be misappropriated in a manner not consistent with its spirit or purpose (DeSanctis and Poole, 1994) because it is "logically malleable" (Moor, 1985; 2001).

What is however, most important is the development of ethically-conscious human beings, who would not be inclined to use IT unethically, irrespective of the punishment severity. For this, there needs to be sound moral education as part of primary and secondary socialization. Our prescription of making children aware of such unethical

issues is due to our finding that even among college students (our sample), the propensity of unethical behavior (or even the intention of unethical behavior) is quite high.

Limitations of the Study

Like every other study, this study has its limitations too. We discuss the limitations of this study one by one.

The first limitation of this study is in the fact that there is a certain problem with using the case based scenario. The case scenarios, while they are beneficial in manipulating variables, are still short on realism. The scenarios, while they depicted possible situations that could have occurred in real life, still are of a somewhat contrived nature. Furthermore, since it is difficult to trace actual behavior, this research used a retrospective measure (how many times the student behaved in this way previously). The measure of behavior was at best indirect, because it assumed that an individual who had acted unethically in the past would also do so in the future with the same frequency. While this may be a reasonable assumption, it may not always be true, especially if students have faced any problems for their past unethical behavior.

The second limitation is in the neglect of a large set of individual factors that may be deemed very important in this context. Factors like gender, age, socioeconomic status, all may be important individual predictors of unethical behavior. For example, in the case scenario of hacking into the computer, the student might be more inclined to make the grade change so as to get the job, if the student comes from a low socio-economic background where the priority of getting a good job is high.

The third limitation of this study is in the fact that it ignores the contextual differences of individuals who are unethically using IT. While the case scenarios provide manipulated contextual conditions, there are various other contextual factors that are left out. Especially, for unethical IT use, a core concern in today's organizations, organizational factors such as organizational practices, mandates, and culture can be deemed to be an important consideration. Especially, there are many factors such as organizational ethical climate (Victor and Cullen, 1988) that become important considerations.

Next, this study concentrates on only two possible instances of unethical behavior. Unethical use of IT can assume many forms like hacking, intellectual property violation, spoofing, plagiarism, deception, and so on. This research is limited in the fact that there are various other types of unethical use that it ignores. We call for future research to extend this model into the realms of other kinds of unethical behavior.

.

Chapter 8 - Contribution and Future Implications

Contribution

This research contributes to existing IS literature in multiple ways. Based on multiple theoretical perspectives, *it is one of the first attempts to develop a comprehensive theoretical model of unethical IT use* based on a wide range of factors: individual, philosophical, social, and technological. To the best of our knowledge, such an extensive model of unethical usage of IT has not been proposed and empirically tested in previous IS literature. This research thus contributes greatly to our overall understanding of unethical IT use.

The second contribution of this research is specifically to the area of IS security. Instances of such unethical usage of IT have become a major security concern (Haines and Leonard, 2007). While a core focus of IS security literature has been devoted to understand and address such security issues through a technological lens (Siponen and Oinas-Kukkonen, 2007), little research till date has been devoted to understanding, especially from an ethical theory perspective, as to why individuals indulge in using IT unethically. In fact, in a recent review of the IS security literature, Siponen and Oinas-Kukkonen (2007) noted that one of the major areas left largely unexplored in the IS security literature has been the relevance and application of the philosophical theories of ethics. In order to address this existing gap, this research, grounded in the philosophical theories of ethics, *develops and tests a general conceptual model of why individuals use IT unethically*. Unraveling the driving factors behind such attitude would shed light on this security concern stemming from the unethical use of IT (Haines and Leonard, 2007).

As a third contribution, this research adds to the literature on IS ethics. Since the focus of the research is to explain the factors influencing unethical use of IT, it adds to this gradually emerging field. Specifically, the attempts in this research to incorporate a wide range of factors in order to provide a new lens to analyze and judge ethical aspects of various IS behavioral phenomena. Furthermore, this research addresses a serious drawback noted by Laudon (1995): the lack of a philosophical base in studying phenomena related to IS ethics. This research, by drawing on the philosophical theories of ethics, addresses this issue.

As a fourth contribution, this research drives home the idea that technology actually may give rise to unethical behavior. In doing so, this research adds to the literature on information ethics that has been steadily growing, trying to understand the moral implications of technology. This research highlights the idea that there are certain characteristics of technology that actually may give rise to unethical behavior. This research delineates that lack of traceability offered by technology could help in unethical behavior. In doing so, this research adds to the literature on information ethics by trying to understand the moral implications of technology. While technology may inherently be amoral, there are certain characteristics that are appropriable in that they could be used to help unethical behavior. This research takes a step toward understanding such characteristics of technology and how they are influential in affecting unethical behavior.

Future Implications

The research also points to numerous implications for future research. The first implication for future research is to test and (in)validate the model across various contexts, samples and behaviors. Additionally, it would be interesting to run comparative

studies between samples (on same behaviors) and between behaviors (on same samples). For example, do software piracy perceptions differ between students and professionals?

The second implication for future research is to understand whether other factors could be important in influencing unethical IT use. For example, it could be the case that demographics (age, gender etc.) could influence unethical IT use. Also, other factors such as psychological orientation and personality types could be important influencers of such behavior. Future research can attempt to address these factors and see how they affect unethical IT use, thus building a more comprehensive model.

The third implication of future research could be to find a different theoretical grounding for explaining unethical use of IT. This research tries to take a TPB approach, but there could be others. A limitation of the research is inherent because of the use of the TPB model where intent is used to predict actual behavior. Due to random factors not included in the model, this might not be the case always. Hence, other theoretical lenses used to understand the phenomenon may be used so as to overcome this limitation. For example, the motivational model (Vallerand, 1997) could be used to predict human unethical behavior using IT.

The fourth implication of future research is to include group unethical behavior using IT. The model is a first step toward a greater understanding of the factors involving unethical IT use. Though it is discussed at an individual level, it can be adapted to the case of group behaviors (e.g. a team of hackers) of unethical IT use by factoring in the group dynamics.

Fifth, unethical issues such as online deception have plagued the e-commerce environment (Grazioli and Jarvenpaa, 2003). In tying the issues of IS ethics to e-

commerce and potential unethical behavior by the concerned parties (sellers and buyers) therein, future research could produce a rich literature base which would considerably enable our idea of business ethics and its implementation in an online market environment.

Another important area of future research would be to investigate unethical use of IT from a different perspective other than deontological and consequentialist ethics. What are the perspectives that should be employed? One fruitful line of research could understand the individual being a virtuous agent rather than being an agent who subscribes to the universalist perspectives of ethics. Virtue ethics (O'Neill, 1996; Hursthouse, 1999), does not judge the ethicality of actions but rather the ethicality of individuals. Virtue ethics draws from the works of Aristotle, who described certain attributes that individuals should have in terms of virtues such as courage, honesty, compassion, and the like. While the main focus of act-based ethical theories (i.e., consequentialism and deontology) is on actions themselves, the focus of virtue ethics is how one can be a good person. The main argument of virtue ethics is that a virtuous individual undertakes actions that are morally correct, in contrast to deontology and utilitarianism (consequentialism) that hold that an individual who undertakes a morally correct action (according to the espoused principles) is morally correct. *Virtue ethics propounds the idea that we should be good persons as opposed to just doing good acts*, famously echoed by the philosopher Nietzsche when he wrote that the future world needed better philosophers, not better philosophy (Nietzsche 1886/1969). This framework of unethical use of IT could be extended to incorporate the notion of virtue ethics, where individuals who are situated within a community of practice can be

understood to be use technology ethically or unethically according to the community of practice the individual is in. While some modern philosophers (e.g., O'Neill, 1996) have attempted to unite the virtue based perspective to other ethical standpoints such as deontology, the field of philosophical ethics still holds that these theories are radically different from each other. Hence, investigating this phenomenon in terms of individual virtues would be an interesting endeavor. In other words the scope of analysis shifts from the focus of action to the individual.

An especially prolific perspective of future research is to investigate this model within the context of different countries and cultures. There is a strong line of reasoning for this. Prior research has argued that culture has a strong influence on ethical perceptions and decision-making (e.g. Robertson and Fadill, 1999; Husted, 1999; Lu et al., 1999; Vitell et al., 1993; Ahmed et al., 2003; Husted, 2000). Husted (2000) quotes Hofsetde (1997) when he defines culture as the "collective programming of the mind which distinguishes the members of one group or category of people from another" (Hofstede 1997: 260). Based on the arguments present here, we can safely conclude that culture has an important effect on individual ethical perception and decision-making. Towing this line, we can thus conclude that culture has a strong influence on individual unethical behavior. In particular, perceptions of what is ethical are determined, to a great extent by the cultural environment surrounding the individual. There is, in fact some evidence in past research to support this claim. Traphagan and Griffith (1998) show that culture might be a factor making a difference in software piracy (a typical case of unethical use of IT) amongst different countries in Europe. Husted (2000) mention that any "policy recommendations that do not take culture into account will be incomplete".

For example, not all countries put the same amount of emphasis on intellectual property rights. Western cultural values of liberalism are much in coherence with the intellectual property rights (Steidlmeier, 1993). Swinyard et al. (1990) show that there is a difference in perceptions of software piracy between Singaporean and US students. A lot of culture-related works in the field of business have been based on Hofstede's (1984; 1997) typology of cultures: power distance, individualism, masculinity and uncertainty avoidance. Of this typology, the individualism and collectivism dimensions have attracted the greatest attention in subsequent research (Roberston and Fadil, 1999). Furthermore, past research (e.g. Husted, 2000) found that only the individualism-collectivism dimension of culture was important in influencing software piracy, a typical case of unethical usage of IT. Hence investigating this model in terms of greater individualistic and collectivistic cultures are appropriate future endeavors. For example, in case of highly collectivist cultures, individual practices assume less importance and group practices assume more importance. Sharing between the in-group assumes more importance in the collectivist cultures and also the tolerance between in-group members is more important. As long as an act is acceptable within an in-group, it becomes acceptable to the individual to a great extent. However, this is not so in the case of the individualistic cultures. In an individualistic society, the acceptability of an act for an individual does not necessarily relate to the in-groups idea about the act. Individual voice attains more importance. Because of this, individuals in such a culture are more aware of violation of others, in terms of privacy, accuracy, property and access. As opposed to it, in collectivist cultures, acceptance of ethical behavior is generally decided by the consensus of the in-group and if such violation is deemed acceptable within the in-group,

it would most likely be OK for any individual within the in-group to undertake such behavior. At another level, it has been noted by Hofstede (1997) that socioeconomic status of a country strongly correlates to the individualistic and collectivistic dimensions of culture. Typically, countries that are wealthier tend to be more individualistic (Husted, 2000). A greater economic affluence implies existence of greater resources that enable acts to be carried out in an ethical manner. For example, in a richer economy, more individuals have enough money to afford the expensive licensed version of software, rather than a pirated one.

The entire point of the arguments presented above is to highlight that various facets of culture may have an important influence on individual perceptions of unethical behavior, and consequently, on their unethical behavior itself. Thus it remains to be empirically seen whether various facets of culture do indeed have a strong influence on unethical behavior and we call upon future research to investigate this phenomenon.

Finally, we call upon a new perspective of ethical thought that has gained importance in recent years, to investigate this phenomenon. This is the postmodern ethical perspective (e.g. Bauman, 1989; 1993) that has criticized the universal principles of ethicality (deontology and consequentialism) on many grounds.

What is postmodern ethics? Faigley (1992, cf. Markel, 1997) provides the following description:

"…there is nothing outside contingent discourses to which a discourse of values can be grounded—no eternal truths, no universal human experience, no universal human rights, no overriding narrative of human progress. This assumption carries many radical implications. The foundational concepts associated with artistic judgment such as

"universal value" and "intrinsic merit," with science such as "truth" and "objectivity," and with ethics and law such as "rights" and "freedoms" suddenly have no meaning outside of particular discourse and are deeply involved in the qualities they are alleged to be describing objectively (p. 8)."

As this description shows, postmodernists undermine the authority of reason (and thus address the problems faced by the universal perspectives of ethics), remarking that any universal principle, such as deontology and consequentialism can never guide any [ethical] decision-making endeavor (Mumby, 1997). This is because they represent "totalitarian" ways of ethical approach and understand ethicality in terms of achieving consensus (Mumby, 1997, Lyotard, 1984), which is of "outmoded and suspect value" (Lyotard, 1984: 66). Any attempt at achieving ethicality through consensus (i.e. consistent adherence to universal principles of ethical conduct) is perilous because it does not really factor in actual concerns of end users and practitioners (Kilduff and Mehra, 1997).

Postmodern ethicists reject the rational worldview propounded by the universal theories of ethics (Bauman, 1989). The postmodernist argument posits that there cannot be any notion of universal knowledge (Remenyi et al., 1997). So, according to postmodernist ethics, what we think as objectively true or accept to be morally right stems from nothing but a subjective understanding of persons and contexts (Mannheim, 1936; Berger and Luckman, 1967) as the core aim of ethics is to not to provide any overarching principles of ethicality but to achieve improvements in localized human settings for short periods of time (Beck et al., 1994, cf. Yuthas and Dillard, 1999). In other words the same principles of ethics become irrelevant across different nations,

customs, cultures, and situational contexts (e.g. the deontological principle, *do not kill*, becomes irrelevant in a war). In fact, one of the core motivations of the postmodern movement has been to remove the narrow and overtly simplistic understanding of complex social processes (Rosenau, 1992), such as unethical use of IT, which have been subjected to much criticism (Kilduff, 1993).

Not surprisingly, the focus of ethical analysis in postmodern ethics is the individual because morality can never be achieved through any implementation of a universal rule perspective; morality is generated from inside the individual through an enactment of individual moral impulse (Bauman, 1993). Rather than the understanding of what is "good" and "true" as being universally agreed upon, to the postmodernist they are subjective (depending on the individual) and are conditioned by each individual's unique set of afflictions (Weiss, 2000). Since the real world is often a product of human consciousness (Becker and Niehaves, 2007), ethicality within a postmodern perspective is a product of individual human emotions and impulses. It does not consider that human beings are ethical due to the fact that they follow any preordained truths or principles (such as deontology and consequentialism) (Bauman, 1993). In this way postmodern ethics directly attacks deontology and consequentialism that rely on such universal assumptions to truth and reality. In the context of unethical use of IT, because the postmodern approach to ethics is always strongly rooted in a relative and subjective understanding—which requires a consideration of the individual's preferences and the context of an action—this approach radically differs from a merely objective subscription of the universal ethical theories. Given that the focus of postmodern ethics is on the individual and begins with the implementation of the involvement of a key player in the

social process (Kilduff and Mehra, 1997), it motivates us to shift our ethical focus to the user of IT and not to his/her actions or outside factors that ordain him/her to act in a certain way.

The entire rationale of presenting the above discussion is to give the reader a sense of how unethical use of IT can be understood from the postmodern perspective and the advantages of following this line of thought. It is a radically different approach from the one we take in this research and calls upon the use of distinctly different epistemologies in order to investigate this phenomenon. While this research has taken a positivist approach to dissecting the phenomenon of unethical use of IT, such a postmodern perspective would necessitate an interpretive or even a critical social perspective. This is a very fruitful line of future research.

References

Ahmed, M. M., K. Y. Chung, and J. W. Eichenseher (2003) "Business Students' Perception of Ethics and Moral Judgment: A Cross-Cultural Study," *Journal of Business Ethics* (43) pp. 89-102.

Ajzen, I. (1991) "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50) 2, pp. 179-211.

Ajzen, I. and M. Fishbein (1977) "Attitude-behavior relations: A theoretical analysis and review of empirical research," *Psychological Bulletin* (84) pp. 888-918.

Al-Rafee, S. and T. P. Cronan (2006) "Digital Piracy: Factors that Influence Attitude Toward Behavior," *Journal of Business Ethics* (63) 3, pp. 237-259.

Andersson, L. M. and T. S. Bateman (1997) "Cynicism in the workplace: Some causes and effects," *Journal of Organizational Behavior* (18) pp. 449–469.

Anscombe, G. E. M. (1958) "Modern Moral Philosophy," *Philosophy* (33) pp. 1-19.

Armitage, C. J. and M. Conner (2001) "Efficacy of the Theory of Planned Behaviour: a meta-analytic review.," *The British journal of social psychology* (40) 4, pp. 471-499.

Aulakh, P. S. and E. F. Gencturk (2000) "International principal–agent relationships—control, governance and performance," *Industrial Marketing Management* (29) pp. 521–538.

Bagchi, K. and G. Udo (2003) "An Analysis of the Growth of Computer and Internet Security Breaches by " *Communications of the Association for Information Systems* (12) pp. 684-700.

Bagozzi, R. P. and Y. Yi (1991) "Multitrait–multimethod matrices in consumer research," *Journal of Consumer Research* (17) pp. 426–439.

Banerjee, D., T. P. Cronan, and T. W. Jones (1998) "Modeling IT ethics: A study in situational ethics," *MIS Quarterly* (22) 1, pp. 31-60.

Baron, D. (2002) "Private Ordering on the Internet: The eBay Community of Traders," *Business and Politics* (4) 3.

Bauman, Z. (1989) *Modernity and the Holocaust*. Ithaca, NY: Cornell University Press.

Bauman, Z. (1993) *Postmodern Ethics*. Malden, MA: Blackwell Publishing.

Beck, L. and I. Ajzen (1991) "Predicting dishonest actions using the theory of planned behavior.," *Journal of Research in Personality* (25) pp. 285–301.

Beck, U., A. Giddens, and S. Lash (1994) *Reflexive modernization*. Stanford: Stanford University Press.

Becker, J. and B. Niehaves (2007) "Epistemological perspectives on IS research: a framework for analysing and systematizing epistemological assumptions," *Information Systems Journal* (17) 2, pp. 197-214.

Bentham, J. (1789/1970) *An Introduction to the Principles of Morals and Legislation*. New York, NY: Methuen.

Bentler, P. M. and C. P. Chou. (1988) "Practical issues in structural modeling," in J. S. Long (Ed.) *Common Problems/Proper Solutions, Avoiding Error in Quantitative Research.*, Newbury Park, CA: Sage Publications, pp. 161–192.

Berger, P. and T. Luckmann (1967) *The social construction of reality: A treatise in the sociology of knowledge*. New York: Doubleday.

Bynum, T. W. (2001) "Computer ethics: Its birth and its future," *Ethics and Information Technology* (3) 2, pp. 109-112.

Campbell, D. T. and D. Fiske (1959) "Convergent and discriminant validation by the multitrait–multimethod matrix," *Psychological Bulletin* (56) pp. 81–105.

Cappel, J. J. and J. C. Windsor (2000) "Ethical decision making: A comparison of computer-supported and face-to-face group," *Journal of Business Ethics* (28) 2, pp. 95-107.

Chatterjee, S. (2005) "A Model Of Unethical Usage Of Information Technology." *Americas Conference on Information Systems, Omaha, Nebraska, 2005*.

Chatterjee, S. (2007) "Ethical Behavior in Technology Mediated Communication," in M. Quigley (Ed.) *Encyclopedia of Information Ethics and Security*, Hershey, PA: Idea Group Reference.

Chatterjee, S., S. Sarker, and M. Fuller (Forthcoming) "A Deontological Approach to Collaboration Ethics: The Design of Building Blocks for Ethical Collaboration Processes," *Journal of the Association for Information Systems*.

Chiles, T. H. and J. F. McMackin (1996) "Integrating variable risk preferences, trust, and transaction cost economics," *Academy of Management. The Academy of Management Review* (21) 1, pp. 73-99.

Chin, W. W. (1998) "Issues and opinion on structural equation modeling," *MIS Quarterly* (22) 1, pp. VII-XVI.

Chin, W. W., B. L. Marcolin, and P. R. Newsted (2003) "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion / adoption study," *Information Systems Research* (14) 2, pp. 189-217.

Chiou, J.-S., C.-y. Huang, and H.-h. Lee (2005) "The Antecedents of Music Piracy Attitudes and Intentions," *Journal of Business Ethics* (57) 2, pp. 161-174.

Christensen, A. L. and M. M. Eining (1991) "Factors Influencing Software Piracy: Implications for Accountants," *Journal of Information Systems* (5) 1, pp. 67-80.

Cohen, J. (1988) *Statistical Power Analysis for the Behavioral Sciences, 2nd ed.* Hillsdale, NJ: Lawrence Erlbaum.

Compeau, D. R. and C. A. Higgins (1995a) "Application of social cognitive theory to training for computer skills," *Information Systems Research* (6) 2, pp. 118-133.

Compeau, D. R. and C. A. Higgins (1995b) "Computer self-efficacy: Development of a measure and initial test," *MIS Quarterly* (19) 2, pp. 189-211.

Conner, K. R. and R. P. Rumelt (1991) "Software Piracy: An Analysis of Protection Strategies," *Management Science* (37) 2, pp. 125-139.

Cullen, J. B., K. P. Parboteeah, and B. Victor (2003) "The effects of ethical climates on organizational commitment: A two-study analysis," *Journal of Business Ethics* (46) 2, pp. 127-141.

Cullen, J. B., B. Victor, and C. Stephens (1989) "An Ethical Weather Report: Assessing the Organization's Ethical Climate," *Organizational Dynamics* (18) 2, pp. 50-62.

Davis, D. L. and S. J. Vitell (1992) "The Ethical Problems, Conflicts and Beliefs of Small Business Information Personnel," *The Journal of Computer Information Systems* (22) 4.

DeSanctis, G. and M. S. Poole (1994) "Capturing the complexity in advanced technology use: Adaptive structuration theory," *Organization Science* (5) 2, pp. 121-147.

Dhillon, G. and J. Backhouse (2000) "Information system security management in the new millennium," *Association for Computing Machinery. Communications of the ACM* (43) 7, pp. 125-128.

Dhillon, G. and G. Torkzadeh (2006) "Value-focused assessment of information system security in organizations," *Information Systems Journal* (16) 3, pp. 293-314.

Diener, E. (1980) *Deindividuation: The absence of self-awareness and self-regulation in group members*. Hillsdale, NJ: Erlbaum.

Donaldson, T. and T. W. Dunfee (1994) "Toward a unified conception of business ethics: Integrative Social Contracts Theory," *Academy of Management. The Academy of Management Review* (19) 2, pp. 252-284.

Ellis, T. S. and D. Griffith (2001) "The evaluation of IT ethical scenarios using a multidimensional scale," *Database for Advances in Information Systems* (32) 1, pp. 75-85.

Ellison, N., R. Heino, and J. Gibbs (2006) "Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment," *Journal of Computer-Mediated Communication* (11) 2, pp. 415-441.

Fabrigar, L. R., R. C. Maccallum, D. T. Wegener, and E. J. Strahan (1999) "Evaluating the use of exploratory factor analysis in psychological research," *Psychological methods* (4) 3, pp. 272-299

Faigley, L. (1992) *Fragments of Rationality: Postmodernity and the Subject of Composition*. Pittsburgh, PA: Univ. of Pittsburgh Press.

Falk, R., F. Miller, and N. B. Miller (1992) *A Primer for Soft Modeling*. Akron, OH: University of Akron Press.

Ferrell, O. C. and L. G. Gresham (1985) "A Contingency Framework for Understanding Ethical Decision Making in Marketing," *Journal of Marketing* (49) 3, pp. 87-96.

Fishbein, M. and I. Ajzen (1975) *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Floridi, L. (1999) "Information ethics: On the philosophical foundation of computer ethics," *Ethics and Information Technology* (1) 1, pp. 37-56.

Floridi, L. (2002) "On the intrinsic value of information objects and the infosphere," *Ethics and Information Technology* (4) 4, pp. 287-304.

Fornell, C. and F. L. Bookstein (1982) "Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory," *Journal of Marketing Research* (19) 4, pp. 440-452.

Fornell, C. and D. F. Larcker (1981) "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research* (18) 1, pp. 39-50.

Fornell, C., P. Lorange, and J. Roos (1990) "The cooperative venture formation process: A latent variable structural modeling approach.," *Management Science* (36) pp. 1246-1255.

Forsyth, D. (1980) "A taxonomy of ethical ideologies," *Journal of Personality and Social Psychology* (39) 1, pp. 175-184.

Forsyth, D. R. (1981) "Moral judgment: The influence of ethical ideology," *Personality and Social Psychology Bulletin* (7) 2, pp. 218-223.

Forsyth, D. R. and R. E. Berger (1982) "The effects of ethical ideology on moral behavior.," *Journal of Social Psychology* (117) 1, pp. 53-56.

Forsyth, D. R., J. L. Nye, and K. Kelley (1988) " Idealism, relativism, and the ethic of caring," *Journal of Psychology: Interdisciplinary and Applied* (122) 3, pp. 243-248.

Forsyth, D. R. and W. R. R. Pope (1984) " Ethical ideology and judgments of social psychological research: Multidimensional analysis.," *Journal of Personality and Social Psychology.* (46) 6, pp. 1365-1375.

Friedman, B. (1996) "Value-Sensitive Design," *Interactions* (3) 6, pp. 16-23.

Friedman, B. and P. H. Kahn (2003) "Human values, ethics, and design," in J. A. Jacko and A. Sears (Eds.) *The Human-Computer Interaction Handbook*, Mahwah, NJ: Lawrence Erlbaum Associates, pp. 1177-1201.

Friedman, B., P. H. Kahn, and A. Boring (2006) "Value Sensitive Design and Information Systems," in P. Zhang and D. Galletta (Eds.) *Human-Computer Interaction in Management Information Systems: Foundations.*, New York, NY: M.E. Sharpe.

Friedman, B. and H. Nissenbaum (1996) "Bias in computer systems.," *ACM Transactions on Information Systems* (14) 3, pp. 330-347.

Garfinkel, R., R. Gopal, and P. Goes (2002) "Privacy Protection of Binary Confidential Data Against Deterministic, Stochastic, and Insider Threat," *Management Science* (48) 6, pp. 749-764.

Gefen, D. and D. Straub (2005) "A Practical Guide To Factorial Validity Using PLS-Graph: Tutorial And Annotated Example," *Communications of the Association for Information Systems* (16) pp. 91-109.

Ghoshal, S. and P. Moran (1996) "Bad for practice: A critique of the transaction cost theory," *Academy of Management. The Academy of Management Review* (21) 1, pp. 13-47.

Gopal, R. D., S. Bhattacharjee, and G. L. Sanders (2006) "Do Artists Benefit from Online Music Sharing?," *The Journal of Business* (79) 3, pp. 1503-1533.

Gotterbarn, D. W. (2001) “Software Engineering Ethics,” in J. Marciniak (Ed.) *Encyclopedia of Software Engineering, 2nd edition*, New York, NY: Wiley-Interscience.

Grazioli, S. and S. L. Jarvenpaa (2000) "Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers," *Systems, Man and Cybernetics, Part A, IEEE Transactions on* (30) 4, pp. 395-410.

Grazioli, S. and S. L. Jarvenpaa (2003) "Deceived," *Association for Computing Machinery. Communications of the ACM* (46) 12, pp. 196-205.

Greene, C. N. and D. W. Organ (1973) "An evaluation of causal models linking the received role with job satisfaction.," *Administrative Science Quarterly* (18) pp. 95–103.

Haines, R. and L. N. K. Leonard (2007) "Individual characteristics and ethical decision-making in an IT context," *Industrial Management + Data Systems* (107) 1, pp. 5-20.

Harrington, S. J. (1996) "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions," *MIS Quarterly* (20) 3, pp. 257-278.

Hofstede, G. (1984) "The cultural relativity of the quality of life concept," *Academy of Management Review* (9) 3, pp. 389-398.

Hofstede, G. (1997) *Cultures and Organizations: Software of the Mind*. New York: McGraw-Hill.

Householder, A., K. Houle, and C. Dougherty (2002) "Computer Attack Trends Challenge Internet Security, Security and Privacy," *Supplement to IEEE Computer*.

Hulland, J. (1999) "Use of partial least squares (PLS) in strategic management research: a review of four recent studies," *Strategic Management Journal* (20) 2, pp. 195-204.

Hunt, S. D. and S. J. Vitell (1986) "A General Theory of Marketing Ethics," *Journal of Macromarketing* (6) 1, pp. 5-16.

Hursthouse, R. (1999) *On Virtue Ethics*. Oxford, UK: Oxford University Press.

Husted, B. W. (1999) "Wealth, culture, and corruption," *Journal of International Business Studies* (30) 2, pp. 339-360.

Husted, B. W. (2000) "The impact of national culture on software piracy," *Journal of Business Ethics* (26) 3, pp. 197-211.

Johnson, D. G. (1994) *Computer Ethics (Second Edition)*. Engelwood Cliffs, NJ: Prentice Hall.

Johnson, D. G. (1997) "Ethics online," *Association for Computing Machinery. Communications of the ACM* (40) 1, pp. 60-65.

Johnson, D. G., J. H. Moor, and H. T. Tavani (2001) "Introduction to Computer Ethics: Philosophy Enquiry," *Ethics and Information Technology* (3) 1, pp. 1-2.

Jones, T. M. (1991) "Ethical Decision Making by Individuals in Organizations: An Issue-Contingent Model," *Academy of Management. The Academy of Management Review* (16) 2, pp. 366-395.

Joreskog, K. G. and H. Wold. (1982) *Systems Under Indirect Observation—Causality Structure Prediction*. Amsterdam, The Netherlands: North-Holland Publishing Company.

Kant, I. (1804/1994) *Ethical Philosophy: Grounding for the Metaphysics of Morals (trans. James W. Ellington)*. Indianapolis: Hackett.

Kesar, S. and S. Rogerson (1998) "Developing ethical practices to minimize computer misuse," *Social Science Computer Review* (16) 3, pp. 240-251.

Kilduff, M. (1993) "Deconstructing organizations," *Academy of Management Review* (18) 1, pp. 13-31.

Kilduff, M. and A. Mehra (1997) "Postmodernism and organizational research," *Academy of Management. The Academy of Management Review* (22) 2, pp. 453-482.

Kuo, F.-Y. and M.-H. Hsu (2001) "Development and validation of ethical computer self-efficacy measure: The case of softlifting," *Journal of Business Ethics* (32) 4, pp. 299-315.

Latour, B. (1987) *Science in Action*. Milton Keynes: Open University Press.

Laudon, K. C. (1995) "Ethical concepts and information technology," *Association for Computing Machinery. Communications of the ACM* (38) 12, pp. 33-39.

Lenman, J. (2000) "Consequentialism and cluelessness," *Philosophy and Public Affairs* (29) pp. 342-370.

Leonard, L. N. K. and T. P. Cronan (2001) "Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences," *Journal of the Association for Information Systems* (1) 12, pp. 1-28.

Limayem, M., M. Khalifa, and W. W. Chin (2004) "Factors Motivating Software Piracy: A Longitudinal Study," *IEEE Transactions on Engineering Management* (51) 4, pp. 414-425.

Lindell, M. K. and D. J. Whitney (2001) "Accounting for Common Method Variance in Cross-Sectional Research Designs," *Journal of Applied Psychology* (86) 1, pp. 114-121.

Loch, K. D. and S. Conger (1996) "Evaluating ethical decision making and computer use," *Association for Computing Machinery. Communications of the ACM* (39) 7, pp. 74-83.

Lu, L.-C., G. M. Rose, and J. G. Blodgett (1999) "The Effects of Cultural Dimensions on Ethical Decision Making in Marketing: An Exploratory Study," *Journal of Business Ethics* (18) 1, pp. 91-105.

Lyotard, J.-F. (1984) *The Postmodern Condition*. Minneapolis: University of Minnesota Press.

MacCallum, R. C. and M. W. Browne (1993) "The Use of Causal Indicators in Covariance Structure Models: Some Practical Issues," *Psychological Bulletin* (114) 3, pp. 533-541.

MacIntyre, A. (1985) *After Virtue*. London: Duckworth.

Mandaric, A., A. Oberweis, and P. Perc. (2005) “Web services-based architecture for reducing behavior and quality uncertainties.” *First International Conference on e-Science and Grid Computing, 2005., 2005*.

Maner, W. (1996) "Unique ethical probelms in information technology," *Science and Engineering Ethics* (2) 2, pp. 137-154.

Mannheim, K. (1936) *Ideology and Utopia*. New York: Brace.

Marakas, G. M., R. D. Johnson, and P. F. Clay (2007) "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time.," *Journal of the Association for Information Systems* (8) 1, pp. 16–46.

Markel, M. (1997) "Ethics and technical communication: A case for foundational approaches," *IEEE Transactions on Professional Communication* (40) 4, pp. 284-298.

Marrett, K. (2004) THE EFFECTS OF COMPUTER SUPPORT, SOCIAL FACILITATION, AND AROUSAL OF SUSPICION ON GROUP DECEPTIVE COMMUNICATION, Florida State University.

Marshall, K. P. (1999) "Has technology introduced new ethical problems?," *Journal of Business Ethics* (19) 1, pp. 81-90.

Mason, R. O. (1986) "Four Ethical Issues of the Information Age," *MIS Quarterly* (10) 1, pp. 5-12.

McPheters, L. R. (1976) "Criminal behavior and the Gains from Crime," *Criminology* (14) pp. 137-152.

Mill, J. S. (1861/1979) *Utilitarianism* Indianapolis, IN: Hackett Publishing.

Moor, J. H. (1985) "What Is Computer Ethics?," *Metaphilosophy* (16) 4, pp. 266-275.

Moor, J. H. (2001) "The future of computer ethics: You ain't seen nothin' yet!," *Ethics and Information Technology* (3) 2, pp. 89-91.

Moore, G. E. (1903) *Principia Ethica*. Cambridge: Cambridge University Press.

Moores, T. and G. Dhillon (2000) "Software Piracy: A View from Hong Kong," *Communications of the ACM* (43) 12, pp. 88-93.

Moores, T. T. and J. C.-J. Chang (2006) "Ethical Decision Making in Software Piracy: Initial Development and Test of a Four-Component Model," *MIS Quarterly* (30) 1, pp. 167-180.

Mumby, D. K. (1997) "Modernism, postmodernism, and communication studies: A rereading of an ongoing debate," *Communication Theory* (7pp. 1-28.

Nagel, T. (ed.) (1988) *War and Massacre. Consequentialism and its Critics*, Oxford: Oxford University Press.

Nietzsche, F. (1873/1995) “On truth and falsity in their extramoral sense (M.A. Mugge, Trans),” in R. Grimm and C. M. Vedia (Eds.) *Philosophical Writings*, New York: The Continuum Publishing Company, pp. 87-99.

Nissenbaum, H. (2004) “Information Technology and Ethics,” in *Berkshire Encyclopedia on Human Computer Interaction*, Great Barrington, MA: Berkshire publishing group.

Nunnally, J. (1978) *Psychometric Theory, 2nd Ed*. New York: McGraw Hill.

O'Neill, O. (1996) *Towards Justice and Virtue: A Constructive Account of Practical Reasoning*. Cambridge, UK: Cambridge University Press.

Organ, D. W. and C. N. Greene (1981) "The effects of formalization on professional involvement: A compensatory process approach.," *Administrative Science Quarterly* (26) pp. 237–252.

Pavlou, P. A., H. Liang, and Y. Xue (2007) "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31) 1, pp. 105-136.

Peace, A. G., F. G. Dennis, and J. Y. L. Thong (2003) "Software piracy in the workplace: A model and empirical test," *Journal of Management Information Systems* (20) 1, pp. 153-177.

Petter, S., D. Straub, and A. Rai (2007) "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (31) 4, pp. 623-656.

Phukan, S. and Dhillon G. " (2001) "Ethical and Intellectual Property Concerns in a Multicultural Global Economy," *EJISDC* (7) 3.

Pinsonneault, A. and N. Heppel (1997) "Anonymity in group support systems research: A new conceptualization, measure, and contingency framework," *Journal of Management Information Systems* (14) 3, pp. 89-108.

Podsakoff, P. M., S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff (2003) "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88) 5, pp. 879–903.

Reidenbach, R. E. and D. P. Robin (1990) "Toward the Development of a Multidimensional Scale for Improving Evaluations of Business Ethics," *Journal of Business Ethics* (9) 8, pp. 639-653.

Reidenbach, R. E., D. P. Robin, and L. Dawson (1991) "An Application and Extension of a Multidimensional Ethics Scale to Selected Marketing Practices and Marketing Groups," *Academy of Marketing Science Journal* (19) 2, pp. 83-92.

Remenyi, D., T. White, and M. Sherwood-Smith (1997) "Information systems management: The need for a post-modern approach," *International Journal of Information Management* (17) 6, pp. 421-435.

Rindfleisch, A. and J. B. Heide (1997) "Transaction cost analysis: Past, present, and future applications," *Journal of Marketing* (61) 4, pp. 30-54.

Riordan, M. H. and O. E. Williamson (1985) "Asset Specificity and Economic Organization," *International Journal of Industrial Organization* (3) 4, pp. 365-368.

Robertson, C. and P. A. Fadil (1999) "Ethical Decision Making in Multinational Organizations: A Culture-Based Model," *Journal of Business Ethics* (19) pp. 385-392.

Robin, D. P., E. W. King, and R. E. Reidenback (1996) "The effect of attorneys' perceived duty to client on their ethical decision making process," *American Business Law Journal* (34) 2, pp. 277-299.

Rogerson, S., J. Weckert, and C. Simpson (2000) "An ethical review of information systems development - The Australian Computer Society's code of ethics and SSADM," *Information Technology & People* (13) 2, pp. 121-136.

Rorty, R. (1989) *Contingency, Irony and Solidarity*. Cambridge: Cambridge University Press.

Rosenau, P. M. (1992) *Post-modernism and the social sciences*. Princeton, NJ: Princeton University Press.

Rosenhead , J. (1989) *Rational Analysis for a Problematic World: Problem Structuring Methods for Complexity, Uncertainty and Conflict.* Chichester: Wiley.

Sandel, M. (1982) *Liberalism and the Limits of Justice*. Cambridge: Cambridge University Press.

Savage, L. J. (1954) *The Foundations of Statistics*. New York, NY: Wiley.

Schoemaker, P. J. H. (1982) "The Expected Utility Model: Its Variants, Purposes, Evidence and Limitations," *Journal of Economic Literature* (20) 2, pp. 529-563.

Schriesheim, C. A. (1979) "The similarity of individual-directed and groupdirected leader behavior descriptions.," *Academy of Management Journal* (22pp. 345–355.

Schultz, E. E. (2002) "A framework for understanding and predicting insider attacks," *Computers & Security* (21) 6, pp. 526-531.

Schweitzer, M. E., L. Ordonez, and B. Douma (2004) "Goal Setting as a Motivator of Unethical Behavior," *Academy of Management Journal* (47) 3, pp. 422-432.

Sen, A. K. (1977) "Rational Fools: A Critique of the Behavioral Foundations of Economic Theory," *Philosophy and Public Affairs* (6) 4, pp. 317-344.

Simon, H. A. (1956) "Rational choice and the structure of the environment," *Psychological Review* (63) 129-138.

Singer, M. (1977) "Actual Consequence Utilitarianism," *Mind* (86) pp. 67-77.

Singhapakdi, A., M. Y. A. Rawwas, J. K. Marta, and M. I. Ahmed (1999) "A cross-cultural study of consumer perceptions about marketing ethics," *The Journal of Consumer Marketing* (16) 3, pp. 257.

Singhapakdi, A., S. J. Vitell, and K. L. Kraft (1996) "Moral intensity and ethical decision-making of marketing professionals," *Journal of Business Research* (36) 3, pp. 245-255.

Siponen, M. T. and H. Oinas-Kukkonen (2007) "A Review of Information Security Issues and Respective Research Contributions," *Database for Advances in Information Systems* (38) 1, pp. 60-80.

Smith, H. J. (2002) "Ethics and Information Systems: Resolving the Quandaries," *Database for Advances in Information Systems* (33) 3.

Spector, P. E. (1987) "Method variance as an artifact in self-reported affect and perceptions at work: Myth or significant problem," *Journal of Applied Psychology* (72) pp. 438–443.

Spinello, R. A. (2002) "The use and abuse of metatags," *Ethics and Information Technology* (4) 1, pp. 23-30.

Stahl, B. C. (2008) "The ethical nature of critical research in information systems," *Information Systems Journal* (18) 2, pp. 137-163.

Steidlmeier, P. (1993) "The Moral Legitimacy of Intellectual Property Claims: American Business and Developing Country Perspectives," *Journal of Business Ethics* (12) pp. 157-164.

Straub, D. W. and R. J. Welke (1998) "Coping with systems risk: Security planning models for management decision making," *MIS Quarterly* (22) 4, pp. 441-469.

Swinyard, W. R., H. Rinne, and A. Keng Kau (1990) "The morality of software piracy: a cross-cultural analysis," *Journal of Business Ethics* (9) 8, pp. 655-664.

Tavani, H. T. (2001) "The state of computer ethics as a philosophical field of inquiry: Some contemporary perspectives, future projections, and current resources," *Ethics and Information Technology* (3) 2, pp. 97-108.

Taylor, C. (1985) *Philosophy and the Human Sciences: Philosophical Papers, Vol II*. Cambridge, UK, : Cambridge University Press.

Taylor, S. and P. A. Todd (1995) "Understanding information technology usage: A test of competing models," *Information Systems Research* (6) 2, pp. 144-176.

Thompson, R., D. W. Barclay, and C. A. Higgins (1995) "The partial least squares approach to causal modeling: Personal computer adoption and use as an illustration," *Technology Studies: Special Issue on Research Methodology* (2) 2, pp. 284–324.

Thong, J. Y. L. and C.-S. Yap (1998) "Testing an ethical decision-making theory: The case of softlifting," *Journal of Management Information Systems* (15) 1, pp. 213-227.

Treas (1993) "Money in the bank: Transaction costs and the economic organization of marriage," *American Sociological Review* (58) 5, pp. 723.

Trevino, L. K. (1986) "Ethical Decision Making in Organizations: A Person-Situation Interactionist Model," *Academy of Management. The Academy of Management Review* (11) 3, pp. 601-617.

Vallerand, R. J. (1997) "Toward a hierarchical model of intrinsic and extrinsic motivation," *Advances in Experimental Social Psychology* (29) pp. 271–360.

Victor, B. and J. Cullen (1988) "The Organizational Bases Of Ethical Work Climates," *Administrative Science Quarterly* (33) 1, pp. 101-125.

Vitell, S. J., S. L. Nwachukwu, and J. H. Barnes (1993) "The effects of culture on ethical decision making: an application of Hofstede's typology," *Journal of Business Ethics* (12) pp. 753-760.

Waldron, J. (1995) “Rights,” in R. E. Goodin and P. Pettit (Eds.) *A Companion to Contemporary Political Philosophy*: Blackwell Publishing.

Wallace, K. A. (1999) "Anonymity," *Ethics and Information Technology* (1) 1, pp. 23-35.

Weiss, R. M. (2000) "Taking Science Out of Organization Science: How Would Postmodernism Reconstruct the Analysis of Organizations?," *Organization Science* (11) 6, pp. 709-731.

Whetstone, J. T. (2001) "How virtue fits within business ethics," *Journal of Business Ethics* (33) 2, pp. 101-114.

Williamson, O. (1985) *The economic institutions of capitalism.* New York: Free Press.

Williamson, O. E. (1975) *Markets and hierarchies: analysis and antitrust implications*. New York, NY: Free Press.

Williamson, O. E. (1981) "The Economics of Organization: The Transaction Cost Approach," *American Journal of Sociology* (87pp. 548.

Williamson, O. E. (1993) "Calculativeness, Trust, and Economic Organization," *The Journal of law & economics* (36) 1, pp. 453.

Wold, H. (ed.) (1985) *Partial least squares. Encyclopedia of Statistical Sciences, Vol 6*, New York: Wiley.

Yuthas, K. and J. Dillard (1999) "Ethical Development of Advanced Technology: A Postmodern Stakeholder Perspective," *Journal of Business Ethics* (19) 1, pp. 35-49.

Zhou, L. (2005) "An Empirical Investigation of Deception Behavior in Instant Messaging," *IEEE Transactions on Professional Communication* (48) 2, pp. 147-160.

Zhou, L., J. K. Burgoon, D. P. Twitchell, T. Qin et al. (2004) "A Comparison of Classification Methods for Predicting Deception in Computer-Mediated Communication," *Journal of Management Information Systems* (20) 4, pp. 139-166.

Zimbardo, P. G. (1970) *The Human Choice: Individuation, Reason and Order Vs. Deindividuation, Impulse and Chaos*. Lincoln: University of Nebraska Press.

Zmud, R. (1990) “Opportunities for strategic information manipulation through new information technology,” in J. Fulk and C. Steinfeld (Eds.) *Organizations and Communication Technology*, Newbury Park, CA: Sage, pp. 95-116.

Appendix A

Case scenarios

Case 1
Imagine that you are in your senior year at your university. You have been doing poorly in one of the key courses of your major you are currently taking. You are afraid that your GPA and future prospects will be affected by a bad grade in this course. One day, while you are visiting the office of the course instructor, you accidentally gain access to the password to his website. This website contains the database that stores all the grades for this particular course. As the semester is drawing to a close, you realize that you are heading toward a very low grade in the course. With companies (intending to hire from your major) scheduled to visit the campus next month, you want to be among the strongest candidates in your class (in terms of the grades). Unfortunately, you know that with your current performance in this course, you will not be perceived by employers as a strong candidate compared to your peers. A possibility strikes you. Since you know the password to the professor's website, you can log in to his website (using your personal laptop from home), access the grade database, and actually increase your grades substantially. This will make you a more attractive candidate as compared to the more deserving students from your major. You know that the instructor is ***hardly concerned of security issues*** and would never imagine that somebody might act in this way. ***Thus, if you were to commit this action, you would most likely <u>not</u> be caught***. However, you remember that there was a similar occurrence of unauthorized grade change by a student some years ago (for a course taught by a different professor). The student was caught, and he was dismissed from the university.

Case 2
Imagine that you are in your senior year at your university. You have been doing poorly in one of the key courses of your major you are currently taking. You are afraid that your GPA and future prospects will be affected by a bad grade in this course. One day, while you are visiting the office of the course instructor, you accidentally gain access to the password to his website. This website contains the database that stores all the grades for this particular course. As the semester is drawing to a close, you realize that you are heading toward a very low grade in the course. With companies (intending to hire from your major) scheduled to visit the campus next month, you want to be among the strongest candidates in your class (in terms of the grades). Unfortunately, you know that with your current performance in this course, you will not be perceived by employers as a strong candidate compared to your peers. A possibility strikes you. Since you know the password to the professor's website, you can

log in to his website (using your personal laptop from home), access the grade database, and actually increase your grades substantially. This will make you a more attractive candidate as compared to the more deserving students from your major. However, you know that the professor is very concerned about security issues and has ***extensive technological controls*** (e.g. log and audit files) in place to know of all the accesses to his website and his database. You also know that his TA checks the log and audit files once a week in order to verify whether there has been any unauthorized access of the professor's website and the course grade database. ***Thus, if you were to commit this action, you would most likely be caught***. Furthermore, you remember that there was a similar occurrence of unauthorized grade change by a student some years ago (for the same course taught by the same professor). The student was caught, and he was dismissed from the university.

Case 3

Imagine that you are in your senior year at your university. You have been doing poorly in one of the key courses of your major you are currently taking. You are afraid that your GPA and future prospects will be affected by a bad grade in this course. One day, while you are visiting the office of the course instructor, you accidentally gain access to the password to his website. This website contains the database that stores all the grades for this particular course.

As the semester is drawing to a close, you realize that you are heading toward a very low grade in the course. With companies (intending to hire from your major) scheduled to visit the campus next month, you want to be among the strongest candidates in your class (in terms of the grades). Unfortunately, you know that with your current performance in this course, you will not be perceived by employers as a strong candidate compared to your peers.

A possibility strikes you. Since you know the password to the professor's website, you can log in to his website (using your personal laptop from home), access the grade database, and actually increase your grades substantially. This will make you a more attractive candidate as compared to the more deserving students from your major. You know that the instructor is ***hardly concerned of security issues*** and would never imagine that somebody might have acted as you did. ***Thus, if you were to commit this action, you would most likely <u>not</u> be caught***. Furthermore, you remember that there was a similar occurrence of unauthorized grade change by a student some years ago (for a course taught by a different professor). Though the student was caught, he was let off only with a warning.

Case 4

Imagine that you are in your senior year at your university. You have been doing poorly in one of the key courses of your major you are currently taking. You are afraid that your GPA and future prospects will be affected by a bad grade in this course. One day, while you are visiting the office of the course instructor, you accidentally gain access to the password to his website. This website contains the database that stores all the grades for this particular course.

As the semester is drawing to a close, you realize that you are heading toward a very low grade in the course. With companies (intending to hire from your major) scheduled to visit the campus next month, you want to be among the strongest candidates in your class (in terms of the grades). Unfortunately, you know that with your current performance in this course, you will not be perceived by employers as a strong candidate compared to your peers.

A possibility strikes you. Since you know the password to the professor's website, you can log in to his website (using your personal laptop from home), access the grade database, and actually increase your grades substantially. This will make you a more attractive candidate as compared to the more deserving students from your major. However, you know that the professor is very concerned about security issues and has ***extensive technological controls*** (e.g. log and audit files) in place to know of all the accesses to his website and his database. You also know that his TA checks the log and audit files once a week in order to verify whether there has been any unauthorized access of the professor's website and the course grade database. ***Thus, if you were to commit this action, you would most likely be caught***. However, you remember that there was a similar occurrence of unauthorized grade change by a student some years ago (for a course taught by a different professor). Though the student was caught, he was let off only with a warning.

Case 5

Assume that you currently live in the university dorm. You have an avid interest in music and closely follow the new music albums being released by a certain artist. One of the albums that you want to possess has just been released. However, it is very expensive and given your limited budget as a student, you do not wish to pay for it. However, you realize it is possible to download the songs of the album from an illegal website onto your personal laptop using the Internet.

The dorm you stay in has hi speed wireless network. You can connect to the wireless network from your laptop. You know that the technical group in charge of the wireless network ***does not maintain extensive technological controls*** (e.g. log and audit files) to keep track of all the websites the users (who are connected to the wireless network) are visiting. Neither are there any log or audit files to monitor downloading activities of the users. ***Thus, if you were to download the songs over the Internet, you would most likely not be caught***. However, you know that students who were previously caught downloading music from illegal websites onto their personal computers were severely punished by the

university authorities. They were expelled from the dorm and also the university.

Case 6

Assume that you currently live in the university dorm. You have an avid interest in music and closely follow the new music albums being released by a certain artist. One of the albums that you want to possess has just been released. However, it is very expensive and given your limited budget as a student, you do not wish to pay for it. However, you realize it is possible to download the songs of the album from an illegal website onto your personal laptop using the Internet.

The dorm you stay in has hi speed wireless network. You can connect to the wireless network from your laptop. However, you know that the technical group in charge of the wireless network ***maintains extensive technological controls*** (e.g. log and audit files) that keep track of all the websites the users (who are connected to the wireless network) are visiting. Furthermore, the log and audit files also keep track of the size of the downloads for each user. Since the music files are large, they may easily attract attention of any person monitoring the log files. ***Thus, if you downloaded the songs over the Internet you would most likely be caught***. Furthermore, you know that students who were previously caught downloading music from illegal websites onto their personal computers were severely punished by the university authorities. They were expelled from the dorm and also the university.

Case 7

Assume that you currently live in the university dorm. You have an avid interest in music and closely follow the new music albums being released by a certain artist. One of the albums that you want to possess has just been released. However, it is very expensive and given your limited budget as a student, you do not wish to pay for it. However, you realize it is possible to download the songs of the album from an illegal website onto your personal laptop using the Internet.

The dorm you stay in has hi speed wireless network. You can connect to the wireless network from your laptop. You know that the technical group in charge of the wireless network ***does not maintain any extensive technological controls*** (e.g. log and audit files) to keep track of all the websites the users (who are connected to the wireless network) are visiting. Neither are there any log or audit files to monitor downloading activities of the users. ***Thus, if you were to download the songs from the Internet, you would most likely <u>not</u> be caught***. Furthermore, you know that students who were previously caught downloading music from illegal websites onto their personal computers were let off only with a warning.

Case 8
Assume that you currently live in the university dorm. You have an avid interest in music and closely follow the new music albums being released by a certain artist. One of the albums that you want to possess has just been released. However, it is very expensive and given your limited budget as a student, you do not wish to pay for it. However, you realize it is possible to download the songs of the album from an illegal website onto your personal laptop using the Internet. The dorm you stay in has hi speed wireless network. You can connect to the wireless network from your laptop. However, you know that the technical group in charge of the wireless network ***maintains extensive technological controls*** (e.g. log and audit files) that keep track of all the websites the users (who are connected to the wireless network) are visiting. Furthermore, the log and audit files also keep track of the size of the downloads for each user. Since the music files are large, they may easily attract attention of any person monitoring the log files. ***Thus, if you downloaded the songs from the Internet you would most likely be caught***. However, you know that students who were previously caught downloading music from illegal websites onto their personal computers were let off only with a warning.