Software Piracy in the Workplace: A Model and Empirical Test

A. GRAHAM PEACE, DENNIS F. GALLETTA, AND JAMES Y.L. THONG

A. GRAHAM PEACE is an Assistant Professor of MIS at the College of Business and Economics, West Virginia University. He obtained his Ph.D. in MIS from the University of Pittsburgh in 1995. His current research interests include the ethical issues of software piracy, privacy, censorship and free speech. His articles have appeared in journals such as *Communications of the ACM, Journal of Computer Information Systems,* and *Business & Society Review.*

DENNIS F. GALLETTA is an Associate Professor of Business Administration at the Katz Graduate School of Business, University of Pittsburgh. He obtained his Ph.D. in MIS from the University of Minnesota in 1985, and was named as an AIS Fellow in December 2002. His current research interests include end user behavior, attitude, and performance. He has served on several editorial boards, including that of the *MIS Quarterly, Data Base,* and *Information Systems and e-Business Management.* His articles have appeared in journals such as *Management Science, Information Systems Research, Journal of Management Information Systems, Communications of the ACM, Decision Sciences, Data Base, Information and Management,* and *Accounting, Management, and Information Technologies.*

JAMES Y.L. THONG is an Associate Professor in the Department of Information and Systems Management, School of Business and Management, Hong Kong University of Science and Technology. He received his Ph.D. in information systems from the National University of Singapore. His research interests include IT adoption and implementation, IT in small business, computer ethics, and IS personnel management. He is on the editorial board of *MIS Quarterly,* and has published in *Information Systems Research, Journal of Management Information Systems, International Journal of Human-Computer Studies, European Journal of Information Systems, Journal of Organizational Computing and Electronic Commerce, Information & Management, Omega, Journal of Information Technology, Information Processing & Management, European Journal of Operational Research, IEEE Communications,* and *Telecommunications Policy.*

ABSTRACT: Theft of software and other intellectual property has become one of the most visible problems in computing today. This paper details the development and empirical validation of a model of software piracy by individuals in the workplace. The model was developed from the results of prior research into software piracy, and the reference disciplines of the theory of planned behavior, expected utility theory, and deterrence theory. A survey of 201 respondents was used to test the model. The results indicate that individual attitudes, subjective norms, and perceived behavioral control are significant precursors to the intention to illegally copy software. In addition, punishment severity, punishment certainty, and software cost have direct effects

Journal of Management Information Systems / Summer 2003, Vol. 20, No. 1, pp. 153–177.

0742–1222 / 2003 $9.50 + 0.00.

on the individual's attitude toward software piracy, whereas punishment certainty has a significant effect on perceived behavioral control. Consequently, strategies to reduce software piracy should focus on these factors. The results add to a growing stream of information systems research into illegal software copying behavior and have significant implications for organizations and industry groups aiming to reduce software piracy.

KEY WORDS AND PHRASES: computer ethics, deterrence theory, expected utility theory, software piracy, theory of planned behavior.

ESTIMATES INDICATE THAT THE ILLEGAL COPYING of software is widespread and costs software manufacturers billions of dollars annually, despite the many legislative and enforcement mechanisms that have been developed in the past two decades. Over one-third of all PC software packages installed in 2000 were illegal copies, resulting in an $11.75 billion loss for the software industry [9]. Whereas many industry groups promote the goal of eliminating this illegal activity, the prevalence of personal computers throughout organizations and the ease with which software can be copied make this a relatively simple action to commit and a difficult crime to detect. In more recent years, the Internet has provided a means for software users to easily transport stolen software around the world. The fact that the crime may appear victimless to the perpetrator further complicates matters. The "software pirate" may see the action as causing little harm to a faceless, billion-dollar company. Technical efforts to prevent illegal copying have gained limited success, at best, and in some cases possibly reduced profits of software companies [14, 25]. The problem of intellectual property rights infringement has also spread to the music and motion picture industries, where losses are estimated to be in the billions of dollars [30].

Taking these problems very seriously, industry groups have studied the issue, including the Business Software Alliance (BSA) and the Software and Information Industry Association (SIIA), formed by the merger of the Software Publishers Association (SPA) and the Information Industry Association (IIA). These groups have attempted to combat software piracy through a two-pronged campaign, including education and punishment. By spreading information regarding the immoral nature and the illegality of the act, both organizations are attempting to impact the norms and attitudes of computer users. For example, the BSA offers a free sample corporate policy on its Web site, and the SIIA provides free auditing software, along with many press releases and reports documenting the potential damage of illegal software copying. The second prong involves the aspect of punishment. By advertising their piracy hot lines and the punishments that can be incurred, the BSA and SIIA are raising awareness of the fact that people are caught and punished for this crime. Both organizations are also involved in promoting more stringent and up-to-date laws prohibiting illegal software copying. Individual organizations use similar strategies. Many companies now publish ethical codes of conduct, and punishment for illegal software copying can be severe.

This paper builds on the growing research into the illegal copying of software by developing a software piracy model focusing on the decision-making process of the individual. The model integrates theory and research from a variety of sources and extends previous work based on social psychology constructs to identify factors that lead to the decision to copy software illegally (e.g., [13, 19, 26]). The development of such a model will help to validate or invalidate the actions and strategies of organizations attempting to combat the software piracy problem. In an industry that employs over 2 million people and generates over $140 billion in annual revenues [8], a threat such as software piracy is a major concern. A better understanding of the roles of the individual's attitude, subjective norms, perceived behavioral control, software cost, and punishment factors in the decision to commit software piracy will aid in the development of mechanisms to reduce this illegal practice.

Theoretical Development

Literature Review

THE ILLEGAL COPYING OF SOFTWARE was raised as a major issue of concern in the academic literature in the mid-1980s, when Richard Mason's [35] seminal paper on the four major ethical issues of the information age specifically cited intellectual property rights as a topic deserving greater study. Four years later, Straub and Collins [54] listed software piracy as a key information issue facing managers and suggested potential ways to reduce the problem, such as organization-wide adoption of basic software applications.

Much of the initial research into illegal software copying consisted of descriptive surveys measuring the attitudes and practices of students and professionals. The term *software piracy* was generally used to indicate any illegal software copying activity. Shim and Taylor [48, 49] surveyed both managers and business school faculty and found that 90 percent of business faculty believed that their colleagues copied software illegally and over 50 percent of managers indicated that they had committed software piracy. The surveys also found that younger managers were more prone to practice software piracy than their older counterparts. This is a trend that runs throughout the literature, and indicates that the practice may increase in frequency as these managers replace the older generation. Oz [39], Paradice [40], Solomon and O'Brien [51], and Kievit [31] all found similar results when studying student populations, with Oz reaching the disturbing conclusion that "young professionals have no scruples about copying software illegally" [39, p. 26]. Christensen and Eining [13] found that business students lacked an understanding of the laws regarding copying software. Paradice [40] concluded that it was especially important for management information systems (MIS) managers to make their new employees specifically aware of their departments' ethical corporate policies. In another study, Sims et al. [50] found that males copied software illegally more frequently than females, and younger students were more likely to pirate software than older students. Peace [41], surveying

computer-using professionals, found that 50 percent of the respondents admitted to copying software illegally.

Using an analytical modeling approach, Gopal and Sanders [25] theorized that deterrence measures could be used to increase software manufacturer profits by dissuading individuals from illegally copying software, and found empirical evidence to support their theory. They also determined that preventive measures, such as anti-copying devices, did not positively affect profits. In a later study, the authors concluded that the existence of a domestic software industry is inversely related to piracy rates in a country [26]. The authors argued that enforcement of intellectual property laws is more likely to occur when a domestic software industry exists.

Gopal and Sanders [26] also argued for the continued development of a behavioral model of software piracy activity as a tool for understanding the actions of software pirates. They tested a model developed using demographic and ethical dimensions, and found that it was better suited to a U.S. sample than a sample taken in India. The authors called for additional research with revised models and improved scales, given the importance of the piracy problem. More recently, Gopal and Sanders [27] proposed a strategy for combating piracy using price discrimination.

Applying a different approach than most studies in the IS literature, Thong and Yap [57] utilized an ethical decision-making theory adapted from the marketing literature. The authors found that entry-level information systems (IS) personnel used both deontological and teleological evaluations to arrive at an ethical decision regarding software piracy, and concluded that efforts to encourage ethical behavior in IS personnel should include training in ethical analysis and enforcement of an organizational code of ethics. By themselves, codes of ethics have been found to have no specific effect on illegal software copying behavior [29, 42].

Interestingly, some research has found that illegal software copying may not necessarily be a damaging act to the software industry. Software piracy acts as an alternate distribution stream for software and may lead to an increase in sales, as individuals who may not have been aware of the product through normal distribution channels are exposed to the software. These individuals may eventually purchase the software or encourage others to purchase the software legally. One study found that software piracy may be responsible for more than 80 percent of new software buyers [24]. The software industry, through its actions, clearly does not agree with this claim and the action of software piracy is certainly illegal, if not harmful, in most countries.

In summary, the prior literature on software piracy mainly involved conceptual discussions, analytical modeling, and descriptive surveys, with limited process studies. As software piracy describes the act of an individual illegally copying software, behavioral models that focus on individual decision-making will be suitable avenues for studying the software piracy problem.

Theory of Reasoned Action

A stream of research in social psychology suggests that a person's behavioral intention toward a specific behavior is the major factor in whether or not the individual

will carry out the behavior [3, 21]. Behavioral intention is, in turn, predicted by the individual's attitude toward the behavior and subjective norms. This is referred to as the theory of reasoned action (TRA). The individual's attitude is his or her feelings of favorableness or unfavorableness toward performing the behavior. This attitude is formed by the individual's beliefs of the consequences and outcomes of the behavior. An individual who believes that an action will lead to positive results will have a favorable attitude toward the behavior. This positive attitude will affect intention, which, in turn, will lead to the actual behavior. Subjective norms refer to the individual's perception of the pressures from the social environment, and are often referred to as peer norms. This is the pressure that the individual feels from friends, peers, authority figures, and so on, to perform or not perform the behavior in question. Much support has been found for the predictive ability of this theory [47], although it has also been found lacking in the explanation of ethical decision-making in situations involving computer issues [33].

Christensen and Eining, in a pair of studies [13, 19], utilized TRA with some success in the study of illegal software copying. Attitude toward software piracy and peer norms were found to be directly related to software piracy behavior. Individuals who pirated software appeared to believe that their peers viewed this as an acceptable action and that the act of piracy was not unethical. However, these studies did not utilize a construct for piracy intention; instead they focused on past piracy behavior. The authors concluded with a call for further research into the underlying beliefs that act as precursors to the attitude and peer norm factors.

Theory of Planned Behavior

The theory of planned behavior (TPB) was developed when the factor of perceived behavioral control was added to TRA [1, 7]. TPB posits that behavior is determined by the intention to perform the behavior, which is predicted by three factors: attitude toward the behavior, subjective norms, and perceived behavioral control. TRA provides theoretical justifications for the links from attitude and subjective norms through intention to behavior. The additional factor, perceived behavioral control, is the individual's perception of his or her ability to commit the behavior. A person with a high level of perceived behavioral control has confidence in his or her ability to successfully carry out the action in question. According to TPB, perceived behavioral control is theorized to impact the intention to perform the behavior.

Much research has been done to validate TPB empirically. Armitage and Conner [5] list 185 studies in various domains utilizing the theory, almost all of which found significant supportive evidence. Whereas the original model of TPB posited interaction effects between the factors, research has only revealed the existence of main effects [7].

It should be noted that, in the specific area of technology acceptance, the rival technology acceptance model (TAM) has been found to explain more variance than TPB. However, TPB provides more specific information regarding the factors that users consider when making a decision [36]. Both models explain intention well,

although TAM's focus on the acceptance of technology, as opposed to the behavior in general, makes the model less applicable to this study.

The relative importance of attitude, subjective norms, and perceived behavioral control are expected to vary across situations [1, 7]. Therefore, it is important to examine each specific behavior (such as software piracy) and the significance of each factor in predicting the behavior. For example, perceived behavioral control was found to be a leading factor in the decision to cheat on an exam or shoplift [7], whereas attitude was found to be more important in the decision to lose weight [45] and use information technology [56]. While attitude and peer norms have been shown to be factors in illegal software copying behavior [13, 19], the role of perceived behavioral control has not received adequate attention. Research comparing the efficacy of perceived behavioral control with attitude and peer norms in predicting unethical behavior needs to be carried out.

To summarize the usefulness of TPB as the base for a predictive model of software piracy, several hypotheses can be posited. Turning our attention toward the three antecedents of intention, links have been made between attitude and intention (e.g., [45, 56]), between subjective norms and intention (e.g., [1, 55]), and between perceived behavioral control and intention (e.g., [7]). Therefore, it is proposed that a more positive attitude toward software piracy, a higher level of subjective norms toward committing software piracy, and a higher level of perceived behavioral control will all lead to greater intention to commit software piracy. This leads to the following hypotheses:

H1: A more positive attitude toward software piracy will lead to greater intention to commit software piracy.

H2: A higher level of subjective norms supportive of software piracy will lead to greater intention to commit software piracy.

H3: A higher level of perceived behavioral control will lead to greater intention to commit software piracy.

Ajzen [1] asserted that behavioral beliefs influence attitude toward a behavior. These beliefs link the behavior to a certain outcome. The more positive the outcome, as perceived by the individual, the more positive the individual's attitude toward that behavior. In the case of illegal software copying, expected utility theory and deterrence theory can be used to identify factors that may affect the possible outcomes of the behavior of software piracy.

Expected Utility Theory

Economic issues, such as costs and benefits, are also commonly claimed to be factors in a person's decision-making process. For example, a lack of financial resources has been cited as a reason for illegal software copying behavior (e.g., [51]). Expected utility theory posits that a rational, self-interested individual will choose the course of

action that maximizes his or her expected utility, when faced with risky choices. The individual making the decision weighs the potential outcome of each alternative, taking into account the expected costs and benefits, and the probability of each alternative occurring. The costs[1] and benefits do not necessarily have to be financial in nature; the individual converts noncomparable items (e.g., software cost versus jail time) into comparable measurement units, namely "utils," via a utility function (a mathematical representation of preferences). The alternative with the highest expected outcome is selected [44, 46].

In most cases, computer users have three possible courses of action when faced with a situation in which software can be used: purchase the software, do without the software, or illegally copy the software. It is possible to describe these choices in terms of expected utility theory. In order to do so, it is necessary to determine the costs and benefits involved. In the case of illegal copying, costs result not only from purchasing the software but also from the punishment level and the probability that the punishment will be incurred. The expected utility of illegal copying is the expected benefit gained from the action less the expected cost (calculated using the punishment probability and punishment level). The individual will illegally copy the software when the expected utility of software piracy is greater than the expected utility of not committing software piracy.

Expected utility theory is a fundamental tenet of much of the analytical work undertaken to date in the area of software piracy (e.g., [10, 14, 25, 26]). Either implicitly or explicitly, the factors identified using utility theory have been clearly shown to have an impact on the software piracy decision. In a survey of graduate and undergraduate students, it was found that the leading reason for people to illegally copy software was that the software was too expensive to purchase, indicating that the benefits of purchasing the software were outweighed by the costs [11]. Similarly, material consequences (the perceived value of gains and losses associated with software piracy, including punishment factors) have been found to have a significant effect on illegal software copying behavior [19]. A negative correlation between piracy rate and per capita gross national product (GNP) has also been demonstrated [27]. The lower a country's annual per capita GNP, the higher the rate of software piracy. This is especially pronounced for countries with annual per capita GNP of less than $6,000. The implication is that individuals in very poor countries cannot afford relatively expensive software packages, which leads to higher piracy rates.

These cost factors can be incorporated into the TPB model to provide a more comprehensive view of the individual's decision-making process, when it comes to software piracy. As stated previously, the attitude factor in TPB is posited to have antecedents related to the possible outcomes of the behavior. In the case of software piracy, a major factor identified by expected utility theory is the cost of the software itself. The higher the cost of the software package, the more financially rewarding the act of software piracy becomes. This factor can be included in the TPB framework as an antecedent of attitude. It is posited that a higher software cost will lead to a more positive attitude toward software piracy, as a greater benefit will be obtained through

the illegal copying of the software. Consequently, the following hypothesis can be posited:

H4: Software cost will have a positive effect on attitude toward software piracy.

Simply stated, the higher the cost of the software, the more likely it is that the individual will have a positive attitude toward software piracy. A discussion of expected costs with respect to punishment levels and probability of punishment is closely linked to deterrence theory and appears below.

Deterrence Theory

The punishment probability factor and the punishment level factor described above are referred to in deterrence theory literature as *punishment certainty* and *punishment severity,* respectively (e.g., [58]). As with expected utility theory, deterrence theory proposes that, as punishment certainty and punishment severity are increased, the level of illegal behavior should decrease. In essence, the unwanted behavior can be deterred through the threat of punishment. Ehrlich [17, 18] directly related this theory to economic factors and found that many crimes against property are related to the expected gains of the crime versus the expected costs at the margin, much as is proposed in the previous section. The author found that the rate of some felonies is positively related to estimated gains and negatively related to expected costs. Straub [53] noted that deterrence measures are a useful primary strategy for reducing computer abuse. These findings have a direct bearing on the illegal software copying problem. The low probability of being caught was listed in a recent survey as the seventh most important reason in the decision to illegally copy software [11].

Not only does deterrence theory identify the importance of the punishment certainty and punishment severity in the decision to illegally copy software, it also highlights the importance of cost. A strong correlation has been found to exist between income inequality and crimes against property [18]. This may be due to the fact that those with less income perceive more potential gain from illegally obtaining property than those for whom the cost of obtaining the property legally is relatively lower. In the case of software, the lower the cost of the software package, the less the gain, if it is pirated. The feeling that others can afford to be victims may also be a factor. Once again, Gopal and Sanders's [27] findings regarding piracy rates and per capita GNP lend support to this line of reasoning.

As with software cost above, punishment certainty and punishment severity are variables that directly relate to the expected outcome. Therefore, in the TPB context, it is posited that each of these factors affects the attitude of the individual toward software piracy. As the chances of being caught and the level of punishment increase, the individual's attitude toward software piracy will become less positive. This leads to the following hypotheses:

H5: Punishment severity will have a negative effect on attitude toward software piracy.

H6: Punishment certainty will have a negative effect on attitude toward software piracy.

The perceived behavioral control factor in TPB is determined by control beliefs [1]. These control beliefs relate to the individual's perceptions of the resources and opportunities necessary to commit the act. In the case of software piracy, a limiting factor on the ability to commit piracy successfully is the probability of detection. It is assumed that, in most cases, the individual will perceive that the detection of the software piracy will lead to the action being halted. This possibility of detection limits the individual's ability to illegally copy the software. Therefore, perception of probability of detection (punishment certainty) is predicted to be a control belief affecting the individual's perceived behavioral control. The greater the chance of being caught, the lower the individual's level of perceived behavioral control. This leads to the final hypothesis:

H7: Punishment certainty will have a negative effect on perceived behavioral control.

Summary

Each of the theories discussed above provides valuable insight into the process behind the software piracy behavior of the individual and the factors involved. Using TPB as a framework, this paper integrates these factors together into a software piracy model (see Figure 1). The hypotheses developed above are all represented in the model, as is the nature of each relationship (positive or negative). As can be seen, the TPB framework is extended using the factors identified by expected utility theory and deterrence theory. Each of the factors identified by these theories is included as an antecedent to the attitude factor, as each operates as a behavioral belief related to the potential outcome of the software piracy decision. Punishment certainty is also included as a predictor of perceived behavioral control, as the perceived possibility of being caught is posited to affect the individual's perception of whether or not he or she could commit the action.

Research Methodology

Questionnaire Development

THE SOFTWARE PIRACY MODEL WAS TESTED using data collected from a questionnaire survey. The questionnaire items utilized in this study are presented in Appendix A. In order to avoid a situation in which subjects had differing ideas as to what constitutes piracy, subjects were specifically advised, both in the written instructions on the questionnaire and in the verbal instructions given by the survey administrator, that the term *software piracy* referred to the illegal copying of software in the workplace. No previously validated questionnaire was available for specifically measuring the factors of *attitude toward software piracy, subjective norms, perceived behavioral control,* and

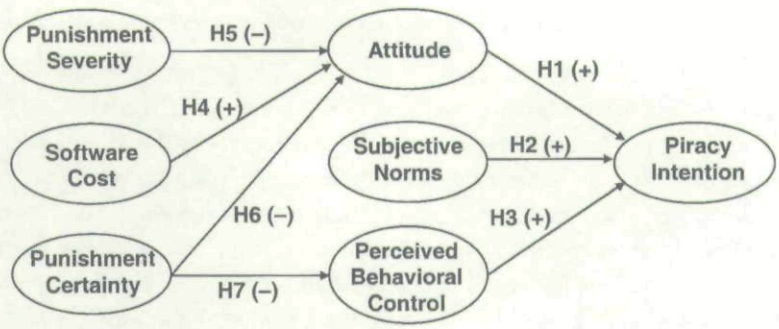

Figure 1. Software Piracy Model

software piracy intention. However, surveys have been carried out with the aim of measuring these TPB constructs in the study of other dishonest behaviors. For example, Beck and Ajzen [7] developed validated questionnaire items to test the applicability of using TPB in predicting individuals' dishonest behavior in the areas of cheating on exams, lying, and shoplifting. Using their instrument as a base, a similar set of items was developed for this study. The original questionnaire items were modified by replacing the dishonest activity previously used with the term *software piracy.* The specific items used to measure perceived behavioral control were also found to be consistent with validated items used in other studies [2].

No previously existing set of items could be identified to measure the individual's perception of *punishment certainty, punishment severity,* or *software cost.* Therefore, new items were developed to measure these constructs. The items did not ask the respondent to give specific figures for these constructs but, instead, attempted to gauge whether the individual perceived the items to be high or low. Specific values are not important in this study, as a specific number perceived as high by one individual may be perceived as low by another.

Due to the need for anonymity in ethics research in order to encourage truthful responses from individuals about their personal activities, we could not identify the respondents for a follow-up survey to determine their predicted software piracy behavior. Further, it would not be easy to measure the predicted software piracy behavior, due to its relatively infrequent occurrence and social desirability effects [59]. Hence, we utilized their software piracy intention as a proxy for their predicted software piracy behavior. While using such a measure is limited by the cross-sectional nature of this study, it does provide an indication of the predicted software piracy behavior in the near future. There is strong support from prior studies on TPB, TRA, and TAM of the link between intention and future behavior (e.g., [4, 16, 47, 55]).

The questionnaire was tested extensively for validity before the actual survey. As described above, previously validated items were slightly modified to create some of the items used in this survey instrument. While the use of previously developed constructs and questionnaire items aids in creating a valid instrument, it does not, in itself, ensure validity [52]. As suggested by Cronbach [15], an iterative review process was undertaken to maximize content validity. This included the distribution of a

preliminary version of the questionnaire to five experts in the academic field and a sample of ten IS professionals. After the items were slightly modified, based on the feedback gathered, the instrument was pilot tested on 38 individuals, resulting in some further minor changes. The final version of the questionnaire was reviewed by five academic and five practitioner experts, and a consensus was reached regarding the clarity and validity of the instrument. Finally, the research variables were extensively tested for reliability and construct validity, upon completion of the entire survey process (see below).

Sample

The survey was conducted on a sample of working adults taking evening classes in the part-time MBA program of a mid-Atlantic U.S. university. All of the respondents were employed at the time of the survey. This group was deemed to be appropriate for the study for a number of reasons. First of all, these individuals had some training with computer systems in their classes and almost all used computers in their everyday workplace and at home. Therefore, they had the necessary skills and technology to commit software piracy, if they so wished, and potentially had access to software that could be copied. Second, these individuals were at a stage in their lives where they were contributing members of society with an understanding of the responsibilities that this entails. They had a good understanding of the purchase cost of software, the business environment in which the software industry operates, and would most likely have some understanding of the potential legal impacts of software piracy. Third, these individuals were working adults who will most likely be the role models and policy-makers of the future. Most of these MBA students were already advancing in their business careers and either already were, or will eventually become, senior managers in their respective organizations. It is important to understand the decision-making process of those individuals who, in the future, will be setting policies regarding such things as intellectual property rights. Last but certainly not least, the sample was readily available.

The survey was completely anonymous (although the respondents were informed that group totals may be released). Instructors in several evening classes distributed the questionnaires, introduced one of the authors to make some brief comments about the study, and invited the students to take some time to complete the surveys before starting class. No rewards were given for participation and no penalties were incurred for not participating. As each student was given a single questionnaire and each returned a questionnaire, there was no way to know who filled in a questionnaire and who chose not to. Of 264 questionnaires that were distributed, 203 were returned completed, yielding a response rate of 76.9 percent. This high response rate can be attributed to the willingness of the students to participate, given the requests of the professors and the convenient nature in which the questionnaire was administered. Due to some missing data on two questionnaires, the data analysis was based on the remaining 201 questionnaires with complete data, yielding a usable response rate of 76.1 percent. Sixty-one percent of the respondents were male and the mean age was

29.1 years. All of the respondents had completed a Bachelors level degree, at a minimum, whereas 96 percent of the respondents used computers on a daily basis.

Results

THE DEMOGRAPHIC DATA SUPPORTED previous surveys on illegal software copying behavior. Fifty-two percent of the total sample admitted to illegally copying software at least once a year, on average, whereas 59.2 percent stated that they had copied software illegally at least once. Interestingly, only 6.5 percent indicated that they knew of an individual in their organization who had been caught copying software illegally, and the mean response to the question "In your opinion, what percentage of people who commit software piracy are caught?" was 8.8 percent.

The software piracy model was tested using partial least squares (PLS). PLS is a powerful second-generation multivariate technique for analyzing causal models involving multiple constructs with multiple observed items [22]. In contrast to factor analysis and traditional regression, which analyze the measurement and structural models separately, PLS assesses both models simultaneously in an optimal fashion. The software utilized was PLS-Graph Version 2.91. All constructs were modeled as reflective measures. The jackknifing procedure (201 resamples with d.f. = 200) was used to estimate the significance of the path coefficients.

Measurement Model

In PLS, analysis of the measurement model involves examining the item reliability, convergent validity, and discriminant validity [23]. Convergent validity is determined by the composite reliability of each construct and the average variance extracted by each construct. As seen in Table 1, the composite reliabilities were above the recommended 0.70 level[2] [28, 38], whereas the average variances extracted were above 0.50 for all constructs. As shown in Table 2, all items loaded highest on their intended constructs with all factor loadings greater than 0.70 (all t-values > 13.56). Hence, the constructs demonstrated more than adequate reliability and convergent validity.

Discriminant validity is the degree to which items differentiate between constructs or measure different constructs. From Table 3, the shared variance (or squared correlation) between any two constructs was less than the average variance extracted by the items measuring the constructs, demonstrating adequate discriminant validity [23]. Further, the confirmatory factor analysis results in Table 2 also provided evidence of discriminant validity.

Structural Model

Following confirmation of acceptable psychometric properties in the measurement model, we examined the analysis of the structural model. In PLS, the predictive power of the structural model is assessed by the R^2 in the endogenous constructs [6, 12].

Table 1. Reliability and Convergent Validity

Construct	Mean	Standard deviation	Composite reliability	Average variance Extracted
Punishment severity			0.95	0.91
Seve1	3.14	1.27		
Seve2	3.27	1.23		
Software cost			0.90	0.74
Cost1	3.98	0.83		
Cost2	3.76	0.96		
Cost3	3.63	0.99		
Punishment certainty			0.92	0.85
Cert1	4.20	1.02		
Cert2	3.82	1.14		
Attitude			0.94	0.79
Att1	2.47	0.98		
Att2	2.62	1.00		
Att3	2.70	0.96		
Att4	2.64	1.04		
Subjective norms			0.87	0.70
Norm1	3.00	1.00		
Norm2	3.44	1.18		
Norm3	3.40	1.12		
Perceived behavioral control			0.92	0.85
PBC1	3.67	1.43		
PBC2	4.05	1.18		
Piracy intention			0.94	0.84
PInt1	3.37	1.31		
PInt2	2.99	1.18		
PInt3	3.29	1.27		

Sixty-five percent of the variance in *software piracy intention,* 24 percent of the variance in *attitude* toward software piracy, and 46 percent of the variance in *perceived behavioral control* were accounted for by the model (see Figure 2). The percentages of variance explained were greater than 10 percent, implying a satisfactory and substantive model [20]. All of the hypotheses were supported with the path coefficients significant at $p < 0.05$.

The results show that software piracy intention is determined by the individual's attitude toward software piracy, subjective norms of his or her peers, and his or her level of perceived behavioral control. Attitude ($\beta = 0.538$) has the strongest effect on software piracy intention, followed by subjective norms ($\beta = 0.275$) and perceived behavioral control ($\beta = 0.136$). When analyzing the relationships between attitude and its predicted antecedents, the results were equally encouraging. Belief of the punishment severity ($\beta = -0.256$) was found to have the strongest relationship with attitude, followed closely by punishment certainty ($\beta = -0.239$) and software cost

Table 2. Loadings and Cross-Loadings

	Punishment severity	Software cost	Punishment certainty	Attitude	Subjective norms	Perceived behavioral PBC	Piracy intention
Seve1	**0.957**	–0.023	0.409	0.359	0.387	0.219	0.336
Seve2	**0.950**	–0.019	0.488	0.334	0.431	0.317	0.323
Cost1	0.005	**0.891**	0.182	0.253	0.245	0.151	0.307
Cost2	–0.046	**0.855**	0.064	0.199	0.119	0.033	0.232
Cost3	–0.024	**0.841**	0.043	0.155	0.066	–0.011	0.196
Cert1	0.383	0.110	**0.920**	0.304	0.455	0.645	0.390
Cert2	0.480	0.120	**0.924**	0.408	0.551	0.606	0.488
Att1	0.311	0.233	0.339	**0.900**	0.570	0.308	0.651
Att2	0.299	0.225	0.324	**0.907**	0.582	0.289	0.659
Att3	0.344	0.201	0.367	**0.883**	0.573	0.303	0.679
Att4	0.339	0.207	0.345	**0.870**	0.522	0.258	0.700
Norm1	0.323	0.102	0.423	0.520	**0.825**	0.324	0.550
Norm2	0.390	0.136	0.485	0.592	**0.843**	0.359	0.549
Norm3	0.358	0.215	0.458	0.470	**0.833**	0.368	0.579
PBC1	0.260	0.008	0.606	0.298	0.412	**0.915**	0.382
PBC2	0.253	0.140	0.640	0.299	0.363	**0.924**	0.402
PInt1	0.320	0.241	0.437	0.700	0.621	0.414	**0.916**
PInt2	0.283	0.295	0.396	0.716	0.555	0.348	**0.913**
PInt3	0.347	0.270	0.477	0.660	0.668	0.408	**0.917**

Note: Figures in boldface are factor loadings on a priori constructs.

Table 3. Discriminant Validity

Construct	1	2	3	4	5	6	7
1. Punishment severity	0.91						
2. Software cost	0.00	0.74					
3. Punishment certainty	0.22	0.02	0.85				
4. Attitude	0.13	0.06	0.15	0.79			
5. Subjective norms	0.18	0.03	0.30	0.40	0.70		
6. Perceived behavioral control	0.08	0.01	0.46	0.11	0.18	0.85	
7. Piracy intention	0.12	0.09	0.23	0.57	0.45	0.18	0.84

Note: Diagonals represent the average variance extracted. Other entries represent the shared variance.

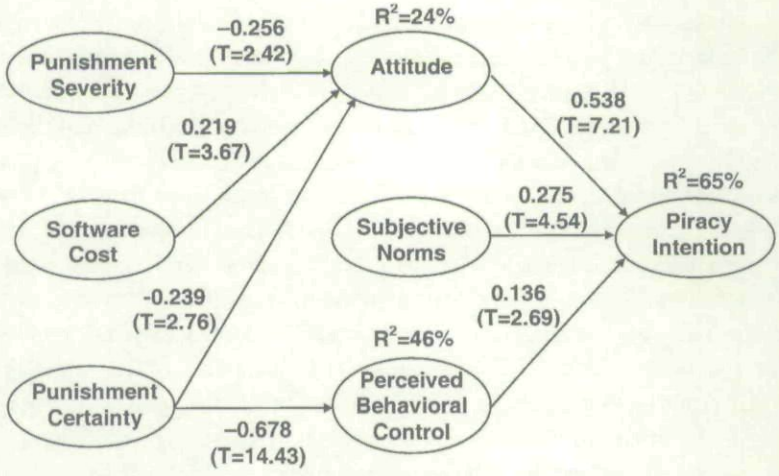

Figure 2. Path Coefficients for Software Piracy Model.

($\beta = 0.219$). Finally, the identification of punishment certainty as a control belief affecting perceived behavioral control was strongly supported ($\beta = -0.678$).

Discussion and Implications

TPB Variables

FOR ORGANIZATIONS, THE RESULTS IMPLY that the factors identified by TPB can be manipulated to yield the desired effects. There is much validation for the strategies currently being utilized by the BSA and the SIIA. As stated previously, the BSA, the

SIIA, and other industry groups and individual organizations have clearly attempted to promote an environment that favors anti-software piracy attitudes and behaviors. For example, the BSA provides free sample corporate policies on its Web site. This study provides evidence that such a tactic is a useful tool in fighting unwanted behaviors such as software piracy. An individual's attitude toward software piracy is clearly a precursor to software piracy intention, which leads to software piracy behavior. By altering attitudes toward software piracy, it should be possible to alter the amount of illegal software copying committed. In addition, influencing individuals' attitudes toward software piracy can reinforce the subjective norms of their peers. Individuals whose peers view software piracy as unethical or illegal tend to believe similarly that the act of software piracy is not ethical or legal, and will be less likely to commit the crime.

Punishment Severity and Certainty

There is evidence that punishment can be a tool in the fight against software piracy. Punishment severity and punishment certainty were both significantly related to attitude. Increasing the punishment certainty can also lead to a decrease in software piracy intention through perceived behavioral control. However, one early study found that less than 10 percent of business students believed that software copyright laws were enforced [13], whereas the average respondent in this study indicated that less than 9 percent of software pirates are caught. Exact levels of software piracy detection and prosecution are difficult to determine and require further research, but raising people's perceptions of the levels of punishment certainty and punishment severity should make it possible to reduce their intention to commit software piracy.

Organizations intent on eliminating illegal software copying within their ranks should consider instituting (and publicizing) significant punishments. Software that is available today (such as that available from the BSA or the SIIA) makes it very easy to perform audits of hard disks. This study indicates that creating and maintaining an audit strategy may, indeed, be a deterrent to software piracy. Such policies must be strictly enforced to achieve the desired results. It is the *perception* of punishment certainty and punishment severity that is important. If individuals perceive high levels of these factors, the study indicates that their intentions to commit software piracy will decrease. Simply having the rules on the books will do little to create change, if the rules are not enforced. Punishments should be clearly defined and communicated to the relevant audience.

The strength of the relationship between punishment certainty and perceived behavioral control is worth noting. This indicates that the more likely an individual perceives the chance of being caught, the less the individual perceives himself or herself as having the ability to commit software piracy. This adds support to the role of auditing in the organization. Increasing the chances of being caught clearly reduces the individual's perceived ability to commit the crime and, therefore, reduces software piracy. Of course, auditing requires time and cost, and does not directly contribute to the bottom line. Therefore, it may not be high on an organization's list

of priorities. However, as part of an overall anti-software piracy campaign, its importance cannot be overlooked. The actions of the BSA and the SIIA to publicize their piracy hotlines appear to be appropriate mechanisms for lowering the net utility of illegal software copying.

Software Cost

Software cost also plays an important role in modifying the individual's attitude toward software piracy. If software is very expensive, the perceived benefits of purchasing the software may be outweighed by its cost. The lower the cost of the software package, the less the gain if it is illegally copied. Whereas hardware has demonstrated a significant increase in value for money over time, software may not be viewed in a similar manner by customers constantly faced with operating system and application upgrades and new releases [37].

While currently not part of the strategy of organizations such as the BSA and the SIIA, the cost factor may have to be taken into account by developers in setting a price for their software. The findings support suggestions to use price discrimination strategies to reduce illegal software copying [10, 27, 37]. This study supports the view that the higher the cost of software, the more likely it is that the individual will copy the software package illegally. Consequently, in countries with significantly lower per capita GNP, it may make sense to lower prices in an effort to gain customers and reduce software piracy. Other anti-software piracy measures, such as educational campaigns and enforced copyright laws, may also be worthwhile. Whereas copyright laws are developed and promoted in countries with little or no software industry, U.S.-based software companies can institute country-dependent software pricing. The software industry may be missing an important ingredient in their efforts to control illegal software copying. Further research in this area would be useful, to confirm the viability of this strategy.

Theoretical Implications

The PLS analysis shows that all of the hypotheses were supported with significant variance explained, indicating that the proposed model is a useful tool for analyzing the software piracy decision. In particular, the TPB structure is an important part of the software piracy model, and both expected utility theory and deterrence theory prove to be suitable theories for identifying critical antecedents of both attitude toward software piracy and perceived behavioral control. The results of this study show that an integrated model of software piracy based on TPB can be developed with success.

It is interesting to note that attitude toward software piracy is clearly the strongest predictor of software piracy intention. The importance of the factors predicting intention can be expected to vary across situations [1, 7], so it is useful to determine which factors are most important in the specific case of software piracy. Perceived behavioral control had the least impact on piracy intention in the proposed model. The relatively stronger effect of attitude makes it even more important to determine the

factors that predict attitude. Clearly, the individual's attitude toward the act of software piracy is a key factor in his or her intention to copy software illegally, based on the results of this study.

When considering the antecedents of attitude, the relative importance of punishment certainty, punishment severity and software cost were similar. The strong results show that the base TPB model can be expanded and improved through the inclusion of factors predicted by other theories, such as expected utility theory and deterrence theory. Much as TRA has been extended through the inclusion of perceived behavioral control, each of the theories discussed above can benefit from the inclusion of other factors in their particular decision-making models, as each omits important factors that have been found to be useful in other theories. For example, expected utility theory and deterrence theory are shown to identify relevant decision-making factors, including cost and punishment factors, but this study indicates that both theories could be improved through the inclusion of additional constructs, such as attitude and perceived behavioral control. The success and development of each theory in its respective research stream indicates that each can provide useful insight into the software piracy decision-making process of the individual, but none tell the whole story. An integrated approach, using insight from all of the relevant theories, is the best next step in studying illegal software copying.

Limitations and Future Research

The current study has some limitations that should be taken into account. First, "software piracy" is a value-laden phrase that is subject to different interpretations by different individuals. For example, some individuals may consider the use of shareware without payment as piracy whereas others may not. Despite the specific definition given to the participants in the administration of the questionnaire and on the questionnaire itself, this may have been a limitation of this study. However, based on the descriptive statistics, the standard deviations of all the variables were relatively small. Analysis of plots also revealed no significant outliers. Hence, there is no evidence of a systematic bias to the statistical results due to potential different interpretations of software piracy.

Second, 23 percent of the respondents did not complete a questionnaire. Although a possible factor may be the sensitivity of the topic, we believe that the cause of the nonresponses is due more to the voluntary nature of the survey. Even before being told of the topic of the survey, some students declined to take part and used the time to get a drink, read the paper, or prepare for class. Also, the survey was rather long, which may have been a deterrent. We believe that these are the likely reasons for the nonresponses, as opposed to a bias due to the sensitivity of the topic. Further, the number of respondents admitting to software piracy behavior was almost identical to results gained in similar studies, providing some measure of validity.

There are also potential avenues for future research. First, the external validity of this study needs to be verified. The use of working MBA students is appropriate and convenient for testing the model but the results may not be generalizable to propo-

nents of open source software or hackers, for example. In particular, the proposed software piracy model can be tested on respondents from other segments of society to increase the generalizability of the findings. Similarly, different scenarios should be tested to validate the generalizability of the model. For instance, the model can be tested in the context of software piracy at home to verify whether the antecedents identified in this study are still applicable.

Second, the model presented in this paper can be tested in non-U.S. cultures to determine its usefulness in predicting software piracy in those cultures. As stated by Gopal and Sanders [26], there is a need to study the cross-cultural aspects of software piracy. Third, there may be other factors that can contribute to predicting software piracy. If so, it will be useful to integrate them into the proposed model of software piracy. In particular, our proposed software piracy model does not take into account research in the field of moral development. Variables that may be examined include levels of moral development [32], moral intensity [34, 43], and religion [60]. Fourth, a promising avenue of research is to extend the current software piracy model to the blossoming problem of music and movie piracy to learn if the proposed model applies as well in that setting. Finally, although not directly related to this study, the claims by a few researchers that software piracy may facilitate, rather than harm the software industry (e.g., [14, 24]), should be studied further. Exploration of the potential positive network externalities and advertising effects from this illegal activity will help to clarify the true nature of the problem and how it should be handled.

Summary and Conclusion

THIS STUDY REFINES AND BUILDS ON the previous attempts to develop a model of software piracy behavior. Previous research has identified the usefulness of the theory of reasoned action (TRA) as a base model in this area. This study extends that model to include the factor of perceived behavioral control, as posited by the theory of planned behavior (TPB). The proposed software piracy model also continues the process of decomposing the TPB constructs and identifying the belief and control variables that determine the main TPB constructs. Whereas previous studies began this process, this study advances a more complex model that integrates TPB with factors identified from expected utility theory and deterrence theory.

There was significant statistical support for the proposed model, accounting for 65 percent of the variance in software piracy intention. All hypothesized relationships appeared to hold. Software piracy intention was predicted by the individual's attitude toward piracy, subjective norms, and his or her level of perceived behavioral control. Beliefs of the severity of punishment, certainty of punishment, and software cost predicted attitude toward software piracy. Finally, punishment certainty had a negative effect on perceived behavioral control.

The results also provide implications for practice on several fronts. There is new support for the practices (e.g., providing sample corporate policies, piracy hotlines, auditing software, and publicizing significant punishments) of agencies that attempt to foster anti-piracy norms in organizations. Within software-using organizations,

increasing employee awareness of the potential severity and certainty of punishment can lead to decreases in intentions to pirate software. Rules alone may not be enough; there needs to be a perception of enforcement. Finally, from the perspective of vendors, there is evidence that higher-cost software is more likely to be pirated than lower-cost software.

Despite the calls of such prominent IS ethics researchers as Richard Mason [35], research in the area of violation of intellectual property rights has long been conspicuous in its absence. However, recent years have seen the development of a small research stream in the IS literature. A rich agenda lies ahead for investigators who wish to better understand the dynamics of the theft of software and other intellectual property, with an ultimate, yet ambitious goal of reducing the significant losses that continue to occur on a daily basis.

Notes

1. One nonfinancial cost that deserves separate study is that of guilt, not included in this study. Unfortunately, the results have not been encouraging. Logsdon et al. [34] found that software piracy was perceived to be an issue of low moral intensity, where pirates face a high level of tolerance for their actions and feel little guilt. Further, Cheng et al. [11] found that individuals tend to be rational and base their pirating decisions more on the economic parameters of the problem. Finally, following Thong and Yap's [57] findings, an argument could be made that a person driven by deontological (moral) thinking would not commit the action and would, therefore, feel no guilt, whereas a person driven by teleological (utility) thinking would commit the act, if there are greater positive consequences, and be unlikely to feel guilt.

2. According to Barclay et al., "the interpretation of the values [composite reliability] obtained is similar, and the guidelines by Nunnally [38] can be adopted" [6].

References

1. Ajzen, I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50,* 2 (1991), 179–211.

2. Ajzen, I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology, 32,* 4 (2002), 665–683.

3. Ajzen, I., and Fishbein, M. Attitude-behavior relation: A theoretical analysis and review of empirical research. *Psychological Bulletin, 84,* 5 (1977), 888–918.

4. Ajzen, I., and Madden, T.J. Prediction of goal-directed behavior: Attitudes, intentions and perceived behavioral control. *Journal of Experimental Social Psychology, 22,* 5 (1986), 453–474.

5. Armitage, C.J., and Conner, M. The theory of planned behavior. *British Journal of Social Psychology, 40,* 4 (2001), 471–499.

6. Barclay, D.; Higgins, C.; and Thompson, R. The partial least squares approach to causal modeling: Personal computer adoption and use as an illustration. *Technology Studies, 2,* 2 (1995), 285–309.

7. Beck, L., and Ajzen, I. Predicting dishonest actions using the theory of planned behavior. *Journal of Research in Personality, 25,* 3 (1991), 285–301.

8. Business Software Alliance. *Forecasting a Robust Future: An Economic Study of the U.S. Software Industry.* Washington, DC: Business Software Alliance, 1999.

9. Business Software Alliance. *2000 Global Software Piracy Report.* Washington, DC: Business Software Alliance, 2001.

10. Chen, Y., and Png, I.P.L. Software pricing and copyright enforcement: Private vis-à-vis social welfare. In P. De and J. DeGross (eds.), *Proceedings of the Twentieth International Conference on Information Systems.* Atlanta: AIS, 1999, pp. 119–123 (available at aisel.isworld.org).

11. Cheng, H.; Sims, R.; and Teegen, H. To purchase or to pirate software: An empirical study. *Journal of Management Information Systems, 13,* 4 (Spring 1997), 49–60.

12. Chin, W.W. The partial least squares approach for structural equation modeling. In G.A. Marcoulides (ed.), *Modern Methods for Business Research.* Mahwah, NJ: Lawrence Erlbaum, 1998, pp. 295–336.

13. Christensen, A., and Eining, M. Factors influencing software piracy: Implications for accountants. *Journal of Information Systems, 5,* 1 (1991), 67–80.

14. Conner, K.R., and Rumelt, R.P. Software piracy: An analysis of protection strategies. *Management Science, 3,* 2 (1991), 125–139.

15. Cronbach, L. Test validation. In R.L. Thorndike (ed.), *Educational Measurement,* 2d ed. Washington, DC: American Council on Education, 1971.

16. Davis, F.D.; Bagozzi, R.P.; and Warshaw, P.R. User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35,* 8 (1989), 982–1003.

17. Ehrlich, I. Participation in illegitimate activities: A theoretical and empirical investigation. *Journal of Political Economy, 81,* 3 (1973), 521–565.

18. Ehrlich, I. Crime, punishment, and the market for offenses. *Journal of Economic Perspectives, 10,* 1 (Winter 1996), 43–67.

19. Eining, M., and Christensen, A. A psycho-social model of software piracy: The development and test of a model. In R. Dejoie, G. Fowler, and D. Paradice (eds.), *Ethical Issues in Information Systems.* Boston: Boyd & Fraser, 1991, pp. 182–187.

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

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

22. Fornell, C. *A Second Generation of Multivariate Analysis, Methods: Vol. 1.* New York: Praeger, 1982.

23. Fornell, C., and Larcker, D.F. Structural equation models with unobservable variables and measurement errors. *Journal of Marketing Research, 18,* 1 (1981), 39–50.

24. Givon, M.; Mahajan, V.; and Muller, E. Software piracy: Estimation of lost sales and impact on software diffusion. *Journal of Marketing, 59,* 1 (1995), 29–37.

25. Gopal, R., and Sanders, G. Preventive and deterrent controls for software piracy. *Journal of Management Information Systems, 13,* 4 (Spring 1997), 29–47.

26. Gopal, R., and Sanders, G. International software piracy: Analysis of key issues and impacts. *Information Systems Research, 9,* 4 (1998), 380–397.

27. Gopal, R., and Sanders, G. Global software piracy: You can't get blood out of a turnip. *Communications of the ACM, 43,* 9 (2000), 83–89.

28. Hair, J.F., Jr.; Anderson, R.E.; Tatham, R.L.; and Black, W.C. *Multivariate Data Analysis with Readings,* 4th ed. Upper Saddle River, NJ: Prentice Hall, 1995.

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

30. International Intellectual Property Alliance. *USTR 2000 "Special 301" Decisions and IIPA 1998–99 Estimated Trade Losses Due to Copyright Piracy.* Washington, DC: IIPA, 2000.

31. Kievit, K.A. Information systems majors/non-majors and computer ethics. *Journal of Computer Information Systems, 32,* 1 (Fall 1991), 43–49.

32. Kohlberg, L. Stage and sequence: The cognitive development approach to socialization. In D.A. Goslin (ed.), *Handbook of Socialization Theory and Research.* New York: Rand McNally, 1969, pp. 347–480.

33. Loch, K., and Conger, S. Evaluating ethical decision making and computer use. *Communications of the ACM, 39,* 7 (1996), 74–83.

34. Logsdon, J.M.; Thompson, J.K.; and Reid, R.A. Software piracy: Is it related to level of moral judgement? *Journal of Business Ethics, 13,* 11 (1994), 849–857.

35. Mason, R.O. Four ethical issues of the information age. *MIS Quarterly, 10,* 1 (1986), 5–12.

36. Mathieson, K. Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research, 2,* 3 (1991), 173–191.

37. Moores, T., and Dhillon, G. Software piracy: A view from Hong Kong. *Communications of the ACM, 43,* 12 (2000), 88–93.

38. Nunnally, J.C. *Psychometric Theory.* New York: McGraw-Hill, 1978.

39. Oz, E. The attitude of managers-to-be toward software piracy. *OR/MS Today, 17,* 4 (1990), 24–26.

40. Paradice, D.J. Ethical attitudes of entry-level MIS personnel. *Information & Management, 18,* 3 (1990), 143–151.

41. Peace, A.G. Software piracy and computer-using professionals: A survey. *Journal of Computer Information Systems, 38,* 1 (1997), 94–99.

42. Pierce, M.A., and Henry, J.W. Judgements about computer ethics: Do individual, coworker, and company judgements differ? Do company codes make a difference? *Journal of Business Ethics. 28,* 4 (2000), 307–322.

43. Ramakrishna, H.V.; Kini, R.B.; and Vijayaraman, B.S. Shaping of moral intensity regarding software piracy in university students: Immediate community effect. *Journal of Computer Information Systems, 41,* 4 (2001), 47–51.

44. Savage, L.J. *The Foundations of Statistics.* New York: Wiley, 1954.

45. Schifter, D.B., and Ajzen, I. Intention, perceived control and weight loss: An application of the theory of planned behavior. *Journal of Personality and Social Psychology, 49,* 3 (1985), 843–851.

46. Schoemaker, P.J. The expected utility model: Its variants, purposes, evidence and limitations. *Journal of Economic Literature, 20,* 2 (1982), 529–563.

47. Sheppard, B.H.; Hartwick, J.; and Warshaw, P.R. The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research, 15,* 3 (1988), 325–343.

48. Shim, J.P., and Taylor, G.S. Business faculty members' perceptions of unauthorized software copying. *OR/MS Today, 15,* 5 (1988), 30–31.

49. Shim, J.P., and Taylor, G.S. Practicing managers' perception/attitudes toward illegal software copying. *OR/MS Today, 16,* 4 (1989), 30–33.

50. Sims, R.R.; Cheng, H.K.; and Teegen, H. Toward a profile of student software piraters. *Journal of Business Ethics, 15,* 8 (1996), 839–849.

51. Solomon, S.L., and O'Brien, J.A. The effect of demographic factors on attitudes toward software piracy. *Journal of Computer Information Systems, 30,* 3 (1990), 40–46.

52. Straub, D. Validating instruments in MIS research. *MIS Quarterly, 13,* 2 (1989), 147–169.

53. Straub, D. Effective IS security: An empirical study. *Information Systems Research, 1,* 3 (1990), 255–276.

54. Straub, D., and Collins, R.W. Key information issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *MIS Quarterly, 14,* 2 (1990), 143–156.

55. Taylor, S., and Todd, P.A. Assessing IT usage: The role of prior experience. *MIS Quarterly, 19,* 4 (1995), 561–570.

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

57. Thong, J.Y.L., and Yap, C.S. Testing an ethical decision-making theory: The case of softlifting. *Journal of Management Information Systems, 15,* 1 (Summer 1998), 213–237.

58. Tittle, C.R. *Sanctions and Social Deviance: The Question of Deterrence.* New York: Praeger, 1980.

59. Trevino, L.K. Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly, 2,* 2 (1992), 121–136.

60. Wagner, S., and Sanders, G.L. Considerations in ethical decision-making and software piracy. *Journal of Business Ethics, 29,* 1–2 (2001), 161–167.

Appendix A. Questionnaire Items

Punishment severity								
Seve1.	If I were caught committing software piracy, I think the punishment would be:*	VERY HIGH	1	2	3	4	5	VERY LOW
Seve2.	If I were caught committing software piracy, I would be severely punished.*	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE
Software cost								
Cost1.	I feel that software prices today are:*	VERY HIGH	1	2	3	4	5	VERY LOW
Cost2.	In my opinion, software packages today are:	VERY INEXPENSIVE	1	2	3	4	5	VERY EXPENSIVE
Cost3.	If I wanted to buy a piece of software today, it would cost me a lot of money.*	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE
Punishment certainty								
Cert1.	If I committed software piracy, the probability I would be caught is:	VERY LOW	1	2	3	4	5	VERY HIGH
Cert2.	If I committed software piracy, I would probably be caught.	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE

Attitude

Att1.	To me, committing software piracy is:*	GOOD	1	2	3	4	5	BAD
Att2.	To me, committing software piracy is:*	PLEASANT	1	2	3	4	5	UNPLEASANT
Att3.	To me, committing software piracy is:	FOOLISH	1	2	3	4	5	WISE
Att4.	To me, committing software piracy is:	UNATTRACTIVE	1	2	3	4	5	ATTRACTIVE

Subjective norms

Norm1.	If I committed software piracy, most of the people who are important to me would:*	APPROVE	1	2	3	4	5	DISAPPROVE
Norm2.	Most people who are important to me would look down on me if I committed software piracy.	LIKELY	1	2	3	4	5	UNLIKELY
Norm3.	No one who is important to me thinks it is okay to commit software piracy.	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE

Perceived behavioral control

PBC1.	If I want to, I can commit software piracy.*	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE
PBC2.	Technically, for me to commit software piracy is:*	EASY	1	2	3	4	5	DIFFICULT

Piracy intention

PInt1.	I may commit software piracy in the future.*	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE
PInt2.	If I had the opportunity, I would commit software piracy.*	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE
PInt3.	I would never commit software piracy.	STRONGLY AGREE	1	2	3	4	5	STRONGLY DISAGREE

Note: * Reversed scale. All reversed items are reversed again for PLS analysis so as to align with their other measures.