An Application of Deterrence Theory to Software Piracy

By

George E. Higgins
Abby L. Wilson
Brian D. Fell
University of Louisville

Although the research on software piracy is growing, criminologists have not examined the role of deterrence in software piracy. Using data collected from 382 undergraduate students attending a southeastern university, this study examined the role of deterrence in reducing instances of software piracy using a factorial design. The findings from the analysis showed that certainty and not severity was important in reducing software piracy. The study also found that contemporary parts of deterrence theory (i.e., shame and family discovery) were important in deterring software piracy. Policy implications of these findings are discussed.

Keywords: deterrence theory; software piracy; factorial design

INTRODUCTION

Recently, the personal computer became an important instrument for individuals' daily lives (Sieber, 1998). Just as personal computer use has increased, so has use of the computer for criminal and deviant activity (Hinduja, 2003). One form of computer crime is software piracy. Sims, Cheng, and Teegan (1996) defined software piracy as the illegal copying of computer software. Others (Britz, 2004; Straub & Collins, 1990) broadened the definition to the unauthorized copying, distributing, or downloading of copyrighted material. To date, the research on software piracy comes from business, information technology, and, more recently, the fields of criminal justice and criminology. However, the collective understanding of deterring and reducing this behavior has not been thoroughly developed. The behavior was so pervasive that one industry account suggested that 39% of all software on computers throughout the world are pirated copies (Business Software Alliance [BSA], 2003). With the continued growth and reliance on personal computers, software piracy and the deterrence of software piracy have become areas of concern for industry groups, law enforcement, and criminal justice scholars. However, our understanding of this behavior from the perspective of deterrence is not complete.

Our current knowledge about deterring software piracy comes almost exclusively from the information technology literature (Gopal & Sanders, 1997; Peace, Gellatta, & Thong, 2003). Sherizen (1995) advocated that computer crime, including software piracy, should be examined using contemporary deterrence theory measures that include: (a) crime control factors (i.e.,

Journal of Criminal Justice and Popular Culture, 12 (3), 166-184.

certainty and severity of sanctions), (b) risk and profit factors (e.g., previous behavioral activities), (c) individual factors (e.g., low self-control, shame, guilt, and moral beliefs), and (d) crime opportunities (i.e., opportunity cost considerations). These deterrence factors outlined by Sherizen (1995) were consistent with the majority of mainstream deterrence theory studies (e.g., Paternoster, 1987; Yu & Liska, 1993), which have been critical of our understanding of how to reduce criminal behavior. We agree with Sherizen (1995), that the research aimed at deterring software piracy should include these factors. In our view, the existing literature lacks clear contributions for examining these factors in such a way that might help develop a usable knowledge base for reducing instances of software piracy.

The goal of the present study was to contribute to the literature by examining the effect of deterrence measures on software piracy. This was the third study to examine such a link. The strength of this study came from applying criminology's updated version of deterrence theory (Grasmick & Bursik, 1990; Nagin & Paternoster, 1993; Pogarsky, 2002; Tibbetts, 1997) to computer crime (i.e., software piracy) as Sherizen (1995) recommended. It was our belief that the information learned from this contribution could be applied to the software piracy problem.

To make this contribution, the study first presents the scope of the software piracy problem. Second, the study explores the link between software piracy and college students. Third, the study presents deterrence theory and its literature. Fourth, the study presents the methods that were used in this study and the results of our analyses. Fifth, and finally, the study presents conclusions drawn from the results and the policy implications they provide.

Scope of the Software Piracy Problem

Computer software is the product of intellectual endeavors that combine creative ideas and talents from different individuals or groups (e.g., programmers, writers, and graphic artists) and shares the same protections under copyright laws as other works of intellectual property such as books, films, and music. As such, software piracy has been illegal since passage of the 1980 Computer Software Act, an amendment of the 1976 Copyright Act. Sims et al. (1996) defined software piracy as the illegal copying of computer software. The amendment specified that individuals and institutions (e.g., colleges or universities and employees) can be held liable for software piracy, even if the individual unintentionally pirated the software (Im & Koen, 1990). Punishments arising from software piracy include prison time of up to 5 years and maximum fines of $500,000 (Koen & Im, 1997).

Economically, software piracy has resulted in the loss of substantial revenue by the software industry and society. The BSA (2003) reported that software piracy has accounted for an annual $11-12 billion of loss. Shin, Gopal, Sanders, and Whinston (2004) estimated that this was an increase from 1995 of more than 50% of the revenues for the software industry. The BSA (2003) estimated that in 2002 the software industry lost $13 billion. During this same time, software piracy took more than 105,000 jobs, more than $5.3 billion in wages, and more than $1.4 billion in tax revenue.

Due to the pervasiveness of the act, the computer industry has developed trade organizations (e.g., the BSA and Software Information Industry Association) to combat the

practice of software piracy. These organizations have typically used research, lobbying, lawsuits, and educational tactics to increase public awareness of the problem. Importantly, these organizations have published estimates of software piracy from different countries around the world. In 2003, research from the BSA estimated that, globally, 39% of all new software had been pirated. In the same report, the BSA estimated that the software piracy rate was 22% in the United States.

Government officials are also combating software piracy. Specifically, DeFrances (2002) showed that software piracy cases were prosecuted by a little over 2% of all prosecutor offices. While this may seem small, 54% of large prosecutor offices (i.e., prosecutor offices that serve more than 1,000,000 individuals) prosecuted software piracy. However, DeFrances also showed that, for offices of smaller sizes, a steep decline in the prosecution of software piracy cases existed. However, prosecutions declined in these cases due to a lack of resources and not a difference in the value of prosecuting software piracy cases. Nevertheless, DeFrances showed that the government was paying attention to this form of crime and was attempting to combat it through prosecution.

Therefore, software piracy is an important emerging crime that criminologists need to research. Specifically, given that software piracy can lead to prison sentences and/or fines, that it is actively being prosecuted, and that it has several different layers of financial costs, the behavior is a substantial problem in need of deterrence. Sherizen (1995) remarked that:

> there is a need for information security [criminal justice practitioners] to determine how best to change the existing perceptions . . . regarding the risks of getting caught in computer crime activities [including software piracy] as well as the perceived payoffs of such activities. (p 179)

However, a necessary issue in deterring piracy is to determine the most likely software pirates.

Software Piracy and College Students

College students regularly use computers for personal and school-related purposes. In order to reduce the occurrence of software piracy, it is therefore important to understand that the behavior persists among college students (Hinduja, 2001, 2003; Hollinger, 1988; Husted, 2000). A nationwide trade organization survey of students (n = 1,000) found that 89% of students did not pay for the software they used (BSA, 2003).

Early and contemporary software piracy research attempted to profile the collegiate software pirate. Such research indicated that college students are ripe for software piracy because: (a) they were never told what was and was not expected of them with respect to hardware and software use, (b) they were not acquainted with the law, and (c) they were generally confronted with ethical issues (Cook, 1986, 1987). The BSA (2003) supported most of these views from Cook (1986, 1987), and showed that most students did not believe that current university policies about unlicensed software were effective. Hinduja (2003) also supported the view of Cook (1986, 1987) that college students were faced with ethical issues and decisions, and suggested that software pirates were likely to participate in other forms of unethical behavior

such as academic dishonesty. Contemporary research has identified the likely software pirate as a male in his 20s majoring in the liberal arts and who frequently uses a computer (Hinduja, 2001, 2003; Hollinger, 1988; Husted, 2000; Sims et al., 1996).

College students provide some unique issues that warrant the investigation of software piracy. First, college students' software piracy could result in financial costs and negative publicity for colleges and universities. Second, software piracy could be a gateway offense for other forms of computer crime (e.g., cyber stalking or identity theft) or other criminal behavior (Hinduja, 2003). Hinduja (2003) pointed out that these issues suggest the importance of studying software piracy among college students in order to bring about the development of policies to reduce its occurrence.

Theoretical Perspective

The main theoretical perspective used by the criminal justice system to reduce instances of criminal and deviant behavior is deterrence theory. That is, deterrence theory was designed to control criminal behavior (i.e., gain compliance to the law; Tyler & Huo, 2002). Deterrence theory suggests this takes place by identifying, discovering, and properly penalizing individuals who are currently performing criminal behaviors. On the other hand, the criminal justice system threatens individuals not currently performing criminal behaviors with legal sanctions (i.e., the certainty and severity of punishment) in order to control crime.

At this point, it is important to note that there are two forms of deterrence theory—classical and contemporary. Classical deterrence theory assumes that individuals are rational beings. That is, the theory assumes that individuals will perform behaviors they perceive as pleasurable or beneficial and avoid behaviors they perceive as painful or costly. Central to the increase in cost perception is an individual's belief that his or her criminal behavior will be detected (i.e., certainty), will be harshly punished (i.e., severity), and that discovery and detection will occur quickly (i.e., swiftness). Thus, in classical deterrence theory, when the threat of punishment is perceived to be certain, severe, and swift, the perceived cost of a criminal behavior becomes increased, triggering caution in the individual that could result in the individual refraining from performing the behavior and thereby deterring and reducing crime.

To date, existing empirical research has not provided complete support for the classical model of deterrence theory. In particular, two meta-analyses showed that the threat of certainty, rather than severity, has more support (Paternoster, 1987; Yu & Liska, 1993). Importantly, these two meta-analyses considered studies that used retrospective accounts, perceptual research (i.e., research that involves scenarios), and longitudinal research. Additional research found corroborating evidence from these meta-analyses (Grasmick & Bursik, 1990; Nagin, 1998; Nagin & Paternoster, 1991; Piquero & Pogarsky, 2002; Pogarsky, 2002). By demonstrating that certainty rather than severity was the most important deterrent measure, the research has suggested that classical deterrence theory is not a complete enough model to understand what deters individuals from crime.

Contemporary deterrence theory recognized the problems with classical deterrence theory, and suggested modifications to the theory through the addition of other measures that

represent inhibitions and motivations for crime. For instance, Grasmick and Bursik (1990) suggested that the inclusion of conscience measures (i.e., shame, guilt, and embarrassment) would add to our understanding of how to deter individuals from crime. Specifically, Grasmisk and Bursik suggested that an understanding of the level of self-disapproval would demonstrate inhibitory effects on criminal behavior, because of the self-stigmatizing implications they provide. Several studies have shown that shame is a more consistent self-stigma measure than guilt (Blackwell, Grasmick, & Cochran, 1994; Grasmick, Blackwell, & Bursik, 1993; Grasmick, Bursik, & Kinsey, 1991; Piquero & Tibbetts, 1996; Tibbetts, 1997; Tibbetts & Myers, 1999). However, other research has shown that guilt is also a promising self-disapproval and self-stigmatizing measure that may reduce criminal behavior (Nagin & Pogarsky, 2003, 2004; Pogarsky, 2002, 2004).

Others have contributed to the literature by using measures to examine whether an individual's moralistic view of a behavior may be an inhibiting factor in deterrence theory. Bachman, Paternoster, and Ward (1992) argued that believing a behavior to be morally wrong may be an inhibiting factor in the decision-making process. On the other hand, individuals that did not believe a behavior was morally wrong would need the threat of other sanctions to inhibit the behavior. This view of moral beliefs has found support in the deterrence literature (Paternoster, 1987; Paternoster & Simpson, 1996; Piquero & Tibbetts, 1996; Pogarsky, 2002, 2004; Tibbetts, 1997). In addition to the criminological deterrence literature, the software piracy literature has also shown that individuals are likely to perform a behavior when they believe the behavior to be ethical rather than unethical (Higgins, 2005; Wagner & Sanders, 2001).

Grasmick and Bursik (1990) argued that social disapproval is an important inhibiting factor for behavior within the deterrence perspective. For instance, they suggested that the possibility of admired, trusted, or close individuals (e.g., family and friends) discovering criminal behavior might function as punishment that could vary in certainty and severity. In other words, discovery of the act embarrasses the actor. Research has shown that when this form of discovery and embarrassment are anticipated or occur on a state level (i.e., situational level) then this type of embarrassment could inhibit or deter the individual from performing the behavior (Pogarsky, 2002). This view has yet to be extended to software piracy.

Some have developed motivational components for criminal behavior in deterrence theory. For instance, Nagin and Paternoster (1991) showed that individuals who had performed a behavior previously were likely to perform the behavior again in the future, because previous performance of the behavior reduced the effectiveness of inhibitions. Under this view, an individual's personality traits changed to where the prior criminal activity increased the likelihood of future criminal activity. This theoretical basis, as well as previous research, has suggested that past behavior holds important information for deterrence research (Cochran, Wood, Sellers, Wilkerson, & Chamlin, 1998; Nagin & Pogarsky, 2003, 2004; Paternoster, 1986; Paternoster & Piquero, 1995). In the software piracy literature, previous research has shown that prior software pirating behavior increases the likelihood of future software pirating behavior (Higgins & Makin, 2004a, 2004b).

Another motivating measure for criminal behavior includes Gottfredson and Hirschi's (1990) version of low self-control. Specifically, Gottfredson and Hirschi argued that low self-

control is the inability of the individual to resist a temptation toward criminal behavior when an opportunity for it exists. The self-control literature, as well as most of criminology, assumes that individuals with low self-control are likely to participate in risky, impulsive, and nonempathic behaviors, because the behaviors satisfy an individual's desire for thrilling and immediately gratifying behaviors. The self-control theory literature has shown that low self-control is indeed an important measure (Nagin & Paternoster, 1993; Piquero & Tibbetts, 1996; Tibbetts, 1997; Tibbetts & Myers, 1999). In addition, recent software piracy research has also shown that low self-control is an important element in understanding software piracy (Higgins, 2005; Higgins & Makin, 2004a, 2004b).

An additional motivating factor in deterrence research is the role of peer association. Akers (1998) demonstrated that deviant or criminal peer association creates a social learning process that increases the likelihood or inclination for criminal behavior. Deterrence research has not overlooked this link between peer association and criminal behavior. Pogarsky (2002) showed that, in deterrence theory, there is a link between peer association and intentions to drive drunk. In addition, research has also shown there to be a link between peer association and software piracy (Christensen & Eining, 1991; Higgins & Makin, 2004b; Skinner & Fream, 1997).

Although Sherizen (1995) called for criminologists to specifically test the contemporary form of deterrence theory using forms of computer crime that include software piracy, the only tests of deterrence theory and software piracy are found in the information technology literature. Gopal and Sanders (1997) used deterrence theory to examine factors that may reduce software piracy and increase profits. They found that certainty would increase the perception of costs and increase industry profits. An additional study by Peace et al. (2003) examined deterrence theory. However, the Peace et al. study examined the mediating effect attitudes and subjective norms (i.e., the favorable perception that significant others would encourage the behavior) would have for perceived certainty and severity on intentions to pirate software. The study showed that perceived certainty and severity were indeed mediated by attitudes and subjective norms. While these studies are important, they provide limited knowledge about how deterrence theory could be applied to software piracy. Specifically, the studies did not explicitly use the classical parts of deterrence theory and only fragmentally used parts of contemporary deterrence theory. Therefore, a gap in the literature exists concerning the role of deterrence theory in reducing software piracy.

The Present Study

The purpose of the present study was to address a gap in the literature by presenting the first systematic examination of deterrence theory in the context of software piracy. This research contributes to both the deterrence theory literature and the software piracy literature. Regarding the deterrence theory literature, the present study went beyond previous research by examining software piracy. Regarding the software piracy literature, the present study was the first effort to apply criminology's version of deterrence theory to this phenomenon. That is, the present study adds to the literature by explicitly making use of the classical parts of deterrence theory and bringing together its contemporary parts. While this was the third effort to use deterrence theory in the software piracy context, our effort contributed to both sets of literature in important and

complementary ways by performing an original study. Beyond these contributions, the present study also provided college administrators and other policy-makers with important information they could use to reduce instances of software piracy.

METHOD

Sample

After Institutional Review Board and Human Subject Protection review, data for this analysis were collected during the fall 2004 semester. Specifically, the researchers gave a self-report questionnaire to college students at a southeastern university in the United States. The students were from different majors enrolled in two courses that were open to all majors, and four courses that were only open to justice administration majors. The researchers asked students who were present on the day the questionnaire was administered to take part in the study during the class period. The researchers told the students of the voluntary nature of the study, and that all responses were anonymous and confidential. This set of procedures produced 386 surveys. However, after listwise deletion for missing cases, only 382 completed surveys remained for analysis. The median age of the sample was 20 years, with a range from 18 to 40. Fifty-six percent of the sample were female (n = 212), and the remaining 44.5% (n = 170) were male. The sample was 17.7% (n = 68) nonwhite and 81.3% (n = 314) white.

The use of a student sample in some studies of deterrence theory may be problematic, because the students may not perform the types of crimes being studied (Wright, Caspi, Moffitt, & Paternoster, 2004). However, in the present study college students were indeed the proper sample, because previous research has shown that this group of individuals frequently performs acts of software piracy (Hinduja, 2001, 2003; Hollinger, 1988; Husted, 2000).

Factorial Design

The factorial design approach combined the strengths of both experiments and probability sampling. That is, it allowed the researchers to develop unique qualities about a given situation without forcing the researchers to tax their respondents (Rossi & Nock, 1982). In the present study, there were four possible unique combinations (i.e., factors) derived from certainty and severity in the software piracy vignette. Using a vignette format, each student would have to rate all four of the combinations to determine the independent effects of the measures, which would not be very efficient. The factorial design allowed the researchers to infer to this population by randomly assigning the vignettes and the factors to the students. Random assignment for this study was achieved by using a random numbers table.

Important features of our study were the development of a believable scenario, as well as certainty and severity factors. We developed these pieces of our survey in two ways. First, we were informed through the literature review about the measures. Second, we developed our measures through administering a 30-item semi-structured survey, in a pilot study, to a small sample (n = 30) of students (the target population) that were not included in the final sample. Two points of emphasis were made in the semi-structured survey: (a) the hypothetical scenario and (b) the extra-legal sanctions. Students were asked to rate the believability of 10 scenarios and

the factors to be included in the study on an 11-point scale that ranged from *not believable* to *100% believable*.

The students were also asked to provide information concerning the different factors to be included in the scenarios. We were concerned about including the proper levels of each factor in the scenarios so as to not depart too far from the perceptual nature of deterrence theory. The students were asked to rate their perception of the certainty that they would be caught performing the scenarios. The students marked their perception of the certainty of being caught on an 11-point scale that ranged from *not being caught at all* to *100% chance of being caught*. In addition, the students were asked to rate their perception of the severity of the sentences that they would receive if they were caught. The students marked their perception of the severity of offense on an 11-point scale with the following categories: (a) "no fine," (b) "500 dollar fine ," (c) "1,000 dollar fine," (d) "10,000 dollar fine," (e) "no jail or fine," (f) "1 month jail time," (g) "3 months jail time," (h) "6 months jail time," (i) "one year jail time," (j) "three years jail time," and (k) "five years jail time." These categories were in accordance with a range of possible punishment severities taken from current legislation concerning software piracy.

We then chose to use the most believable survey from this pilot group. That is, 75% of the students (n = 23) in the pilot study marked that the following scenario was at least 95% believable:

> You are taking a class that requires a lot of computer homework. The class is important to your success in your major because other classes use the same material, so you want to learn the material and make a good grade in the class. You have all of the computer programs that you need for the class EXCEPT for one. So, you go to the bookstore to purchase the software; however, you cannot afford it. Others in the class have told you that they own the program and would be willing to burn a copy for you.

We then chose to use a range of responses to develop the certainty and severity factors that would be randomly assigned in the scenarios for the students. The pilot study revealed that a range from 20-80% certainty contained 90% (n = 27) of the students' responses about the certainty of being caught for software piracy. The responses from the pilot study revealed that 70% of the students (n = 21) provided responses that ranged between a $500 fine and spending 3 months in jail.

From the pilot study, in our view, we were left with a partially student-generated (i.e., target-population-generated) scenario and set of factors. We chose to minimize the complexity of the survey and to use the end points of our ranges as the factors. This resulted in a 2 (certainty levels) X 2 (severity levels) factorial design. We recognize that some may not concur with our method of selecting the scenario and factors for our study. They could argue that our certainty and severity measures reduce variation in the perception of these measures. However, we felt this procedure was similar to Bouffard's (2002) suggestions for participant-generated information for rational choice and deterrence studies. Therefore, we believed the scenario was relevant to this population.[1] In addition, we felt we had identified a reasonable set of factors that could be varied among the sample for the present study.

Dependent measure. Similar to previous deterrence research (e.g., Pogarsky, 2002), the dependent measure for this study was the students' response to a single item, "What is the likelihood that you would take the software under these circumstances?"[2] The students marked their responses on an 11-point scale that was anchored by the responses *not likely* and *100% likely*. Higher scores on the item reflected a greater likelihood they would perform the act.

Low self-control. The measure of low self-control used in the present study was the 24-item composite scale from Grasmick, Tittle, Bursik, & Arneklev (1993). Response categories for the scale ranged from 1 = *strongly disagree* to 4 = *strongly agree*. Higher scores signaled lower levels of self-control. This scale had an internal consistency of .83, and factor analysis with a scree test showed the scale to be unidimensional, a finding similar to other deterrence and rational choice studies (see Nagin & Paternoster, 1993; Piquero & Tibbetts, 1996).

Extra-legal sanctions. The social- and self-disapproval measures used in the present research were alike. To measure the expected influence of social-disapproval similar to Grasmick and Bursik (1990), the students were asked two questions: "How likely is it that your family would find out that you used a copy of the program in the circumstances described in the scenario?" and "How likely is it that your friends would find out that you used a copy of the program in the circumstances described in the scenario?" The students addressed these questions using an 11-point scale anchored by *not likely* and *likely*. To measure the expected influence of self-disapproval, the students were asked, similar to Pogarsky (2002), "How likely would you feel guilty if you were to use the copy of the program in the circumstances described in the scenario?" and, similar to Paternoster and Piquero (1995), "How likely would you feel shame if you were to use the copy of the program in the circumstances described in the scenario?" The students addressed these questions using an 11-point scale that was anchored by *not likely* and *100% likely*. In addition, as in Bachman et al. (1992), the students addressed the following question: "How morally wrong would it be if you were to use the copy of the program in the circumstances described in the scenario?" The students answered this question using an 11-point scale anchored by *not wrong* and *100% wrong*.

Additional control measures. The students responded to additional control measures that included their self-reports of the number of times they had pirated software before and their percentage friends who had pirated software before, as well as their gender (0 = male, 1 = female), race (1 = white, 0 = nonwhite), and age (an open-ended item).

RESULTS

Table 1 presents descriptive statistics and bivariate correlations for the measures. Not shown in the table is that the distribution of the dependent measure (intentions to pirate software) was not overly skewed (-.75) and did not contain a substantial number of zero responses (10%; n = 38). To be sure the correct analysis was presented, Tobit and Ordinary Least Squares (OLS) regressions were performed and compared. Although not shown, we performed Tobit regression because some deterrence studies (Paternoster & Piquero, 1995; Pogarsky, 2002) used this technique due to substantial zero responses in the dependent measure. The results from the Tobit regression were substantively the same as the OLS, without any changes in direction of the coefficients. Therefore, we decided to present only the correlational analysis and OLS results.

Table 1

Sample Descriptive Statistics and Bivariate Correlations of Measures (*n* = 369)

	Mean	SD	1	2	3	4	5	6	7	8	9	10	11	12	13
1. Intentions	6.52	3.30													
2. Morally Wrong	4.89	3.34	-.41*												
3. Gulity	3.17	3.13	.48*	.67*											
4. Shame	2.99	3.11	-.50*	.65*	.92*										
5. Family Discovery	3.14	3.21	-.42*	.60*	.65*	.67*									
6. Friend Discovery	1.46	2.42	-.38*	.44*	.60*	.62*	.67*								
7. Previous Piracy	1.39	1.71	.25*	-.24*	-.28*	.30*	.32*	-.28*							
8. Peer Association	13.10	8.98	.30*	-.13*	-.18*	-.21*	-.10	-.11*	.16*						
9. Low Self-Control	51.31	8.03	.27*	-.15*	-.21*	-.17*	-.13*	-.12*	.10	.28*					
10. Certainty	1.50	0.50	-.12*	-.08	-.01	.10	-.02	.02	-.00	-.10	-.06				
11. Severity	1.51	0.50	.06	-.12*	-.06	-.06	-.03	-.02	.06	-.01	.08	-.00			
12. Gender	2.26	1.09	-.03	-.17*	-.18*	-.18*	-.22*	-.14*	.21*	.01	.17*	.01	.02		
13. Age	21.45	4.72	-.25*	.15*	.19*	.20*	.06	.23*	-.15*	-.11	-.18*	.05	.02	.06	
14. Ethnicity	0.83	0.38	.07	-.02	-.02	-.01	-.06	-.09	.04	.17*	.12*	-.11*	-.00	.03	-.05

*$p < .05$.

Table 2

Multiple Regression with Intentions to Pirate Software and Independent Measures (*n* = 369)

	b	SE	Beta	Tolerance	VIF
1. Morally Wrong	-.11	.06	-.11	.48	2.07
2. Guilty	-.03	.12	-.02	.31	2.67
3. Shame	-.24*	.12	-.23	.41	2.75
4. Family Discovery	-.15*	.07	-.14	.37	2.65
5. Friend Discovery	-.04	.08	-.03	.47	2.11
6. Previous Piracy	.15	.09	.07	.83	1.19
7. Peer Association	.06*	.02	.15	.84	1.18
8. Low Self-Control	.06*	.02	.15	.83	1.19
9. Certainty	-.68*	.02	-.10	.96	1.03
10. Severity	.10	.28	.02	.96	1.03
11. Gender	-1.11*	.30	-.17	.88	1.13
12. Age	-.05	.38	-.01	.94	1.06
13. Ethnicity	-.13	.07	-.08	.87	1.14
F	16.81*				
R^2	.38				
Adjusted R^2	.36				

Note. VIF = Variance Inflation Factor.

*$p < .05$.

Table 1 shows correlations among the measures. The associations between moral beliefs and guilt ($r = .67$), moral beliefs and shame ($r = .65$), moral beliefs and family discovery ($r = .60$), guilt and family discovery ($r = .65$), family discovery and shame ($r = .67$), friend discovery

and shame (r = .62), and family and friend discovery (r = .67) were all equal to or greater than .60, while the association between guilt and shame (r = .75) had the largest association. The strength of these associations suggested that multicollinearity may have been an issue in these data, and variance inflation factors (VIFs) and tolerance coefficients from OLS were necessary for this analysis. From the classical deterrence theory measures, certainty had a significant negative association, albeit weak, with software piracy (r = -.12), but severity did not have a significant association with software piracy (r = .06). This supported the findings of previous deterrence theory research (e.g., Paternoster, 1987; Yu & Liska, 1993).

Table 2 presents results from the OLS regression analysis that applied classical and contemporary deterrence theory measures to software piracy. These results showed that six measures accounted for 38% of the variance in software piracy. Specifically, the results provided mixed support for the classical deterrence theory perspective, finding that certainty (b = -.68, B = -.10, t = -2.44) but not severity (b = .10, B = .02, t = 0.38) had a negative link with software piracy. Shame also had a negative link with software piracy (b = -.24, B = -.23, t = -1.97), supporting part of the self-disapproval view from contemporary deterrence theory. In addition, the results supported another part of contemporary deterrence theory, showing that family discovery had a negative link (b = -.15, B = -.14, t = -2.12) with software piracy. Gender also had a negative link with software piracy (b = -1.11, B = -.17, t = -3.75), which supported the demographic contention from the software piracy literature that males are significantly different from females with respect to software piracy. That is, females were less likely than males to pirate software. On the other hand, peer association had a positive link (b = .06, B = .15, t = 3.44) with software piracy, supporting the view that this sort of association might motivate the behavior. The view that individuals sought thrills and behaved on impulses that benefited themselves was also supported in the results, with a significant link between low self-control and software piracy (b = .06, B = .15, t = 3.22).

The bivariate correlation analysis suggested that multicollinearity could have been an issue with these data, but the regression analysis did not provide evidence of multicollinearity through the use of VIFs and tolerance. Typically, researchers have viewed VIFs above four and tolerance coefficients below .20 as problematic (Field, 2000). In our analysis, none of the VIFs were above two and none of the tolerance measures approached or were below .20.

DISCUSSION

The purpose of the present study was to address gaps in the literature by presenting the first systematic examination of how deterrence theory can reduce instances of software piracy. In this study, the certainty and severity levels were experimentally manipulated and randomly assigned to students. The results show that certainty had a significantly negative link with software piracy. This finding is consistent with a substantial amount of classical deterrence theory literature (Paternoster, 1987; Piquero & Pogarsky, 2002; Pogarsky, 2002; Sherizen, 1995; Yu & Liska, 1993). This suggests that as certainty increases software piracy decreases, and that the public and private sectors need to develop teams that can more accurately research and implement security measures.

Severity was not an important deterrent in these data, which is also consistent with the literature (Paternoster, 1987). However, this could be due to our measure of severity. While we attempted to allow the participants to provide the most cogent measure of certainty, our method was not without its faults. On the other hand, this result is consistent with previous deterrence theory literature (e.g., Paternoster, 1987; Pogarsky, 2002; Sherizen, 1995). Therefore, we conclude that the deterrent effect from certainty may be more important in reducing software piracy than severity.

In addition to classical deterrence theory measures, the results which show that shame may inhibit software piracy is consistent with previous research (Grasmick, Blackwell, et al., 1993; Grasmick et al., 1991; Piquero & Tibbetts, 1996; Tibbetts, 1997; Tibbetts & Myers, 1999). This measure found shame to be an important self-conscious emotion which may provide a sense of self-disapproval and self-stigma that an individual may find undesirable with respect to software piracy.

Further, the results show that family disapproval had a significant negative link with software piracy. This result supports previous deterrence theory research (Grasmick & Bursik, 1990). Importantly, the result suggests that social disapproval from the family may provide a sense of social stigma that could produce inhibitions toward software piracy.

An important link is present in these data concerning the gender of the individual. Our finding that males are more likely to be software pirates supports previous research (Hinduja, 2001, 2003). This could suggest that a gender gap exists in this form of offending that deserves the attention of future research. Also important are the links that low self-control and peer association have with software piracy. Our results support the contention from Gottfredson and Hirschi (1990) and other empirical research (Higgins, 2005; Higgins & Makin, 2004a, 2004b) that temptation is too much for an individual with low self-control to resist. In addition, the link between peer association and software piracy is consistent with the previous literature (Akers, 1998; Higgins, 2005; Higgins & Makin, 2004a, 2004b).

Furthermore, findings of the current study provide several policy implications for three specific areas: (a) law enforcement, (b) legislative, and (c) organizational. Law enforcement needs to develop proper procedures to detect and investigate these cases to increase the certainty of apprehension. Educational institutions can assist law enforcement if a law is passed that requires them to report every violation. In addition, prosecutor offices need to be trained, equipped, and funded properly, which may occur legislatively, to prosecute software piracy. Organizationally, educational institutions can provide orientation sessions to make students aware of the certainty of software piracy apprehension. In addition, the training process may emphasize the shame that could arise from the detection and prosecution of software piracy. This training may indicate the social embarrassment felt when an offender's family is notified of software piracy infringements and the penalties that come with such criminal behavior. In addition, educational institutions may provide "pop-ups" on students' computers that remind users of these issues after the orientation sessions. At a minimum, educational institutions can provide students with written literature about issues pertaining to software piracy. In essence, we believe there is a culture that thinks software piracy is proper behavior, but if educational

institutions can change this climate to emphasize the criminogenic issues surrounding software piracy, then the behavior may be reduced.

While the present study has found support for various parts of classical and contemporary deterrence theory, the study has limits. First, our measure of severity may have had too little variance for this analysis, which is a limit among factorial surveys of this type. However, while this is a limit, it is not a fatal flaw, partly because we performed a pilot study to allow the participants to somewhat generate the severity and certainty measures in order to preserve some perceptual qualities of the sanctions. Second, the data for this study come from a cross-sectional sample from one university in the southeast, possibly restricting generalizability of the results. However, software piracy is prevalent among students from this type of university. Third, the study only makes use of one software piracy scenario.

Despite its limitations, the present study provides evidence that some parts of classical and contemporary deterrence theory may be used to reduce instances of software piracy. In particular, the study shows that certainty, shame, and family disapproval may be important for reducing instances of software piracy. Further, the study shows that association with peers who pirate software and low self-control are important covariates of software piracy. Future studies that expand the number of scenarios, use different college campuses, and manipulate important emotional components of deterrence will be very useful in understanding how deterrence can reduce software piracy. For now, the present study supports our view, as well as that of Sherizen (1995), that the deterrence theory perspective may be used to reduce instances of computer crime—specifically software piracy.

NOTES

1. The use of scenarios in examining deterrence and rational choice theories has become rather routine (Klepper & Nagin, 1989; Piquero & Tibbetts, 1996; Tibbetts & Gibson, 2002). However, some may argue that this technique may not allow for adequate examination of crime theories (Tibbetts & Gibson, 2002). On the other hand, software piracy scholars such as Shore et al. (2001) have implied that software piracy is a behavior that has subtle complexities that can best be captured using scenarios. In fact, Shore et al. implied that using direct measures of software piracy is likely to result in minimum variation and may be inflated with zeros. In addition, this technique has been successfully used in previous tests that link crime theories to software piracy (Higgins, 2005; Higgins & Makin, 2004a, 2004b).

2. The specific measures for this study can be obtained from the first author on request.

ENDNOTE

George E. Higgins is an Assistant Professor in the Department of Justice Administration at the University of Louisville. He received his Ph.D. in criminology from Indiana University of Pennsylvania in 2001. His most recent publications appear in *Criminal Justice and Behavior*, *Journal of Crime and Justice, Journal of Economic Crime Management*, *Criminal Justice Studies, College Student Journal,* and *Western Criminology Review*. His current research focuses on criminological theory testing and quantitative methods. All correspondence concerning this article should be sent to George E. Higgins, University of Louisville, Department of Justice Administration, Louisville, KY 40292. E-mail address is: gehigg01@gwise.louisville.edu.

Abby L. Wilson is a graduate student in the Department of Justice Administration. She received her Bachelor of Science in Justice Administration from the University of Louisville. Her current interests are environmental crime, criminological theory, and computer crime.

Brian D. Fell is a graduate student in the Department of Justice Administration. He received his Bachelor of Arts in Political Science and Bachelor of Science in Justice Administration from the University of Louisville. His current interests are identity theft, criminological theory, and computer crime.

REFERENCES

Akers, R. (1998). *Social learning and social structure: A general theory of crime and deviance.* Boston: Northeastern University Press.

Bachman, R., Paternoster, R., & Ward, S. (1992). The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law and Society Review, 26*, 343-372.

Blackwell, B. S., Grasmick, H. G., & Cochran, J. K. (1994). Racial differences in perceived sanction threat: Static and dynamic hypotheses. *Journal of Research in Crime and Delinquency*, *31*, 210-224.

Bouffard, J. A. (2002). Methodological and theoretical implications of using subject-generated consequences in tests of rational choice theory. *Justice Quarterly*, *19*, 747-771.

Britz, M. T. (2004). *Computer forensics and cyber crime: An introduction*. Upper Saddle River, NJ: Prentice Hall.

Business Software Alliance (2003). *Software piracy fact sheet.* Retrieved June 10, 2003, from http://www.bsa.org

Christensen, A., & Eining, M. M. (1991, Spring). Factors influencing software piracy: Implications for accountants. *Journal of Information Systems*, *5*, 67-80.

Cochran, J. K., Wood, P. B., Sellers, C. S., Wilkerson, W., & Chamlin, M. B. (1998). Academic dishonesty and low self-control: An empirical test of a general theory of crime. *Deviant Behavior*, *19*, 227-255.

Cook, J. M. (1986). What CS graduates don't learn about security concepts and ethical standards or every company has its share of damn fools. Now every damn fool has access to a computer. *ACM SIGCSE Bulletin*, *18*, 89-95.

Cook, J. M. (1987). Defining ethical and unethical behaviors using departmental regulations and sanctions. *ACM SIGCSE Bulletin*, *19*, 462-468.

DeFrances, C. J. (2002). *Prosecutors in state courts, 2002*. Washington, DC: Bureau of Justice Statistics.

Field, A. (2000). *Discovering statistics using SPSS for windows*. Thousand Oaks, CA: Sage Publications.

Gopal, R. D., & Sanders, L. G. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems*, *13*, 29-47.

Gottfredson, M. R., & Hirschi, T. (1990). A *general theory of crime.* Palo Alto, CA: Stanford University Press.

Grasmick, H. G., Blackwell, B. S., & Bursik, R. J. (1993). Changes in the sex patterning of perceived threats of sanctions. *Law & Society Review*, *27*, 679-705.

Grasmick, H. G., & Bursik, R. J. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law & Society Review*, *24*, 837-861.

Grasmick, H. G., Bursik, R. J., & Kinsey, K. A. (1991). Shame and embarrassment as deterrents to noncompliance with the law: The case of an antilittering campaign. *Environment & Behavior*, *23*, 233-251.

Grasmick, H. G., Tittle, C. R., Bursik, R. J., & Arneklev, B. J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency*, *30*, 5-29.

Higgins, G. E. (2005). Can self-control theory help understand the software piracy problem. *Deviant Behavior*, *26*, 1-24.

Higgins, G. E., & Makin, D. A. (2004a). Does social learning theory condition the effects of low self-control on college students' software piracy? *Journal of Economic Crime Management*, *2*, 1-22.

Higgins, G. E., & Makin, D. A. (2004b). Self-control, deviant peers, and software piracy. *Psychological Reports*, *95*, 921-931.

Hinduja, S. (2001). Correlates of Internet software piracy. *Journal of Contemporary Criminal Justice, 17,* 369-382.

Hinduja, S. (2003). Trends and patterns among online software pirates. *Ethics and Information Technology*, *5*, 49-61.

Hollinger, R. C. (1988). Computer hackers follow a Guttman-like progression. *Sociology and Social Research, 72,* 199-200.

Husted, B. W. (2000). The impact of national culture on software piracy. *Journal of Business Ethics*, *13*, 431-438.

Im, J. H., & Koen, C. (1990). Software piracy and responsibilities of educational institutions. *Information & Management, 18,* 189-194.

Koen, C. M., & Im, J. H. (1997). Software piracy and its legal implications. *Security Journal*, *31*, 265-272.

Klepper, S., & Nagin, D. (1989). Tax compliance and perceptions of the risks of detection and criminal prosecution. *Law & Society Review*, *23*, 209-240.

Nagin, D. S. (1998). Deterrence and incapacitation. In M. H. Tonry (Ed.), *Handbook of crime and punishment* (pp. 345-368). Oxford, United Kingdom: Oxford University Press.

Nagin, D. S., & Paternoster, R. (1991). The preventive effects of the perceived risk of arrest: Testing an expanded conception of deterrence. *Criminology*, *29*, 561-587.

Nagin, D. S., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law & Society Review, 27*, 467-496.

Nagin, D. S., & Pogarsky, G. (2003). An experimental investigation of deterrence: Cheating, self-servicing bias, and impulsivity. *Criminology*, *41*, 167-193.

Nagin, D. S., & Pogarsky, G. (2004). Time and punishment: Delayed consequences and criminal behavior. *Journal of Quantitative Criminology*, *20*, 295-318.

Paternoster, R. (1986). The use of composite scales in perceptual deterrence research: A cautionary note. *Journal of Research in Crime and Delinquency*, *23*, 128-169.

Paternoster, R. (1987). The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues. *Justice Quarterly*, *4*, 173-217.

Paternoster, R., & Piquero, A. (1995). Reconceptualizing deterrence: An empirical test of personal and vicarious experiences. *Journal of Research in Crime and Delinquency*, *32*, 251-286.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review*, *30*, 549-583.

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

Piquero, A. R., & Pogarsky, G. (2002). Beyond Stafford and Warr's reconceptualization of deterrence: Personal and vicarious experiences, impulsivity, and offending behavior. *Journal of Research in Crime and Delinquency, 39*, 153-187.

Piquero, A. R., & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice Quarterly*, *13*, 481-510.

Pogarsky, G. (2002). Identifying 'deterrable' offenders: Implications for research on deterrence. *Justice Quarterly*, *19*, 431-453.

Pogarsky, G. (2004). Projected offending and contemporaneous rule-violation. *Criminology*, *42*, 111-136.

Rossi, P. H., & Nock, S. L. (1982). *Measuring social judgments: The factorial survey approach*. Beverly Hills, CA: Sage Publications.

Sherizen, S. (1995). Can computer crime be deterred? *Security Journal*, *6*, 177-181.

Shin, S. K., Gopal, R. D., Sanders, G. L., & Whinston, A. (2004). Global software piracy revisted. *Communications of the ACM*, *47*, 103-107.

Shore, B., Venkatachalam, A. R., Solorzano, E., Burn, J. M., Hassan, S. Z., & Janczewski, L. J. (2001). Softlifiting and piracy: Behavior across cultures. *Technology in Society*, *23*, 563-581.

Sieber, U. (1998). *Legal aspects of computer-related crime in the information society* (COMCRIME—Study prepared for the European Commission). Wurzburg, Germany: University of Wurzburg. Retrieved September 5, 2004, from http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html

Sims, R., Cheng, H. K., & Teegan, H. (1996). Toward a profile of student software pirates. *Journal of Business Ethics*, *15*, 839-849.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, *34*, 495-518.

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

Tibbetts, S. G. (1997). Shame and rational choice in offending decisions. *Criminal Justice and Behavior*, *24*, 234-255.

Tibbetts, S. G., & Gibson, C. L. (2002). Individual propensities and rational decision-making: Recent findings and promising approaches. In A. R. Piquero & S. G. Tibbetts (Eds.), *Rational choice and criminal behavior: Recent research and future challanges* (pp. 3-24). New York: Routledge Press.

Tibbetts, S. G., & Myers, D. L. (1999). Low self-control, rational choice, and student test cheating. *American Journal of Criminal Justice*, *23*, 179-200.

Tyler, T., & Huo, Y. J. (2002). *Trust in the law: Encouraging public cooperation with the police and the courts*. New York: Russell Sage Foundation.

Wagner, S. C., & Sanders, L. (2001). Considerations in ethical decision-making software piracy. *Journal of Business Ethics*, *29*, 161-168.

Wright, B. R. E., Caspi, A., Moffitt, T. E., & Paternoster, R. (2004). Does the perceived risk of punishment deter criminally prone individuals? Rational choice, self-control, and crime. *Journal of Research in Crime and Delinquency*, *41*, 180-213.

Yu, J., & Liska, A. (1993). The certainty of punishment: A reference group effect and its functional form. *Criminology*, *31*, 447-464.