New Insights for an Old Problem: Explaining Software Piracy through Neutralization Theory

Mikko Siponen
Department of Information Processing Science
University of Oulu
mikko.siponen@oulu.fi

Anthony Vance
Information Systems Department
Brigham Young University
anthony@vance.name

Robert Willison
Department of Informatics
Copenhagen Business School
rw.inf@cbs.dk

Abstract

Software piracy continues to be a major economic concern for organizations. Given the widespread nature of the problem, software piracy has received attention from IS scholars. Previous research indicates that neutralization—a form of rationalization—can help to explain software piracy intentions. However, a knowledge gap exists in our understanding about which techniques of neutralization contribute most to software piracy intentions. To address this gap, we advance a model that explains the effects of neutralization techniques on software piracy intentions. For greater explanatory power, we also include formal sanctions, shame, and moral beliefs in our model. Empirical results (n=183) show that neutralization techniques “appeal to higher loyalties” and “condemnation of the condemners” strongly predict software piracy intentions. In addition, shame and moral beliefs are also strong predictors. These findings suggest that anti-piracy efforts should involve educational interventions aimed at addressing these two neutralization techniques, rather than relying on formal sanctions.

1. Introduction

Surveys all around the world report that people commonly use unauthorized software copies [22, 21]. Because the unauthorized copying of software is widespread, companies claim that such behavior constitutes a serious economic threat [21]. It is perhaps no surprise, therefore, that this problem has received considerable academic attention. To be more precise, researchers have advanced a number of models in order to explain why individuals copy software, (for a review of these see [43]). Previous research indicates that neutralization – a form of rationalization by an individual – can help to explain software piracy intention [30]. This is an important contribution as the neutralization techniques do not only offer a new approach to understand and tackle illegal copying, but they also may explain why sanctions do not deter the copying of software. Unfortunately, previous research has not addressed which neutralization technique contributes most to software piracy [30]. Without this information, it is difficult to design the necessary campaign and education interventions that attempt to overcome these neutralization techniques. To address this gap in the research, we advance a model which encompasses the relationship between each element of deterrence theory and intention to copy software. We also include formal sanctions, since the neutralization theory suggests that formal sanctions may not be as effective when neutralization techniques are applied by an individual. In addition, shame and moral belief are also introduced to the model. The model is tested using students (n=183). Our results are of relevance for scholars and anti-piracy organizations. For anti-piracy organizations, de-neutralizing neutralization techniques offer a new understanding as to why people may copy software. Neutralization techniques may also help anti-piracy organizations to understand why formal sanctions do not deter. For scholars, this research offers new research avenues with regard to how peoples’ intentions may be affected by strategies attempting to de-neutralize the neutralization techniques.

2. Theoretical Model Development

Before discussing the theoretical development of our model, we present the model and hypotheses in Figure 1. The model consists of two well-known criminological theories: neutralization techniques [48] and deterrence [35].

2.1 Neutralization Theory

In their seminal text ‘Techniques of Neutralization: A Theory of Delinquency’, Sykes and Matza’s [48] starting point is to question the idea of a delinquent sub-culture which rejects the values of ‘respectable society’ and maintains its own values and norms. Sykes and Matza contend that delinquents do, show signs of conformity to society. If apprehended a delinquent may experience feelings of guilt and shame, and often respect those individuals who conform to the
social order. The paradoxical question which subsequently emerges is ‘Why does delinquency occur if delinquents demonstrate signs of conformity?’ The answer, according to Sykes and Matza is that much delinquency is underpinned by rationalizations, which are used by delinquents to justify their own criminal behavior. It is argued that these rationalizations help to mitigate and diminish the influence of internalized norms and social controls which are designed to inhibit deviant behavior. Sykes and Matza call these rationalizations ‘techniques of neutralization’ and advance five types, which include ‘condemnation of the condemners’, ‘denial of injury’, ‘appeal to higher loyalties’, ‘denial of responsibility’, and ‘denial of the victim’. Aside from the five identified by Sykes and Matza, additional research has identified two other techniques entitled ‘metaphor of the ledger’ [14] and the ‘defense of necessity’ [50].

While several studies have followed Sykes and Matza’s research by applying the techniques of neutralization to examine delinquency [29] it has been noted that the rationalization process is thought to occur in the commission of all forms of crime [18]. Indeed the application of neutralization techniques have been used to research a diverse range of crimes including drug-use [39], hate crimes [7], tax evasion [51] and deer poaching [14]. Given this diverse application we believe that neutralization techniques can be applied to help understand software piracy. The seven techniques will now be described.

The ‘condemnation of the condemners’ involves the situation where the delinquent moves the focus of attention away from his/her own actions to those who oppose such behavior. The delinquent may, therefore, view the police as ‘brutal’, ‘corrupt’ or ‘stupid’. Hence, by criticizing the behavior of the ‘condemners’ the delinquent is able to dissipate the wrongfulness of his/her actions. Thus we can hypothesize:

\[ H_1: \text{Condemning the condemners positively affects the intention to commit software piracy.} \]

The ‘denial of injury’ involves the delinquent rationalizing their behavior in a manner which diminishes the perceived harm of their actions. Hence auto-theft may simply be viewed as ‘borrowing’ and vandalism as mere ‘mischief’. Thus we can hypothesize:

\[ H_2: \text{Denial of injury positively affects intention to commit software piracy.} \]

As noted, other researchers have added to Sykes and Matza’s five techniques. In their study of deer poaching, Eliason and Dodder [14] incorporate the ‘metaphor of the ledger’. With this technique an individual compares their criminal (a debit) with their law-abiding behavior (a credit). The individual, therefore, rationalizes the former as insignificant and justified compared with their overall honest actions. Eliason and Dodder provide the example of a convicted poacher who argued ‘In 40 years of hunting all sorts of game and as in as many states I have never
broken the law of any state except one’ [14, p. 244]. Thus we can hypothesize:

H3: The metaphor of the ledger positively affects intention to commit software piracy.

The ‘appeal to higher loyalties’ encompasses the situation where a criminal is able to diminish the external and internal controls, imposed by society, through acquiescing to the demands of a smaller group. Sykes and Matza provide the example of a delinquent who aligns his loyalty to a gang as opposed to the dominant social order. Neutralizations such as ‘never squeal on a friend’ or ‘always help a buddy’ may, therefore, be invoked. Thus we can hypothesize:

H4: The appeal to higher loyalties positively affects intention to commit software piracy.

Another relatively recent addition to the techniques of neutralization is the ‘defense of necessity’ [50]. This technique enables the individual to rationalize their criminal behavior as unavoidable. The white-collar criminal may argue that while certain business activities may be illegal (e.g. bribes), they are commonplace and necessary to remain competitive. Thus we can hypothesize:

H5: Defense of necessity positively affects intention to commit software piracy.

The ‘denial of responsibility’ involves the delinquent rationalizing his/her actions in a manner which absolves them of responsibility and therefore avoids possible censure from others. Sykes and Matza provide the example of how a juvenile may perceive themselves as a ‘billiard ball’, propelled into criminal behavior as a result of bad company and unloving parents. Thus we can hypothesize:

H6: Denial of responsibility positively affects intention to commit software piracy.

Finally, offenders may further rationalize their actions through the ‘denial of victim’. In this instance, if the victim is ‘absent, unknown, or a vague abstraction’, the offender is able to marginalize the existence of the victim and therefore rationalize the crime as victimless. A variation of this specific technique acknowledges how an offender may rationalize their actions in a manner which, rather than believing their actions to be wrong, justifies their behavior to be ‘rightful retaliation’ or ‘punishment’. As Sykes and Matza state, “By a subtle alchemy the delinquent moves himself into the position of an avenger and the victim is transformed into the wrong-doer” [48, p. 668]. Thus we can hypothesize:

H7: Denial of the victim positively affects intention to commit software piracy.

At first glance it may appear that the techniques of neutralization have little to offer in terms of insights into software piracy. However, a closer inspection may prove otherwise. For example, could it not be imagined that with regard to the ‘defense of necessity’ a student may argue ‘I really need the software to do my college work, but couldn’t afford it, so I copied it from a friend’? Or, what about the ‘denial of the victim’? It has been noted if the victim is ‘physically absent, unknown, or a vague abstraction’ then the offender is able to marginalize the victim and hence perceive the crime to be victimless. Is software piracy not a good example of this technique?

2.2 Deterrence Theory

While we expect the influence of neutralization techniques to be substantial in the context of software piracy, we also recognize that situational factors are likely to exert influence on a person’s decision to commit software piracy. In the field of Criminology, one of the leading theories to explain such situational factors is Deterrence Theory [35]. In fact, modern deterrence theory was developed in part to explain situational elements in the context of a crime that fell outside the scope of dispositional or relational theories like differential association [11, 5]. Thus, the use of Neutralization Techniques and deterrence theories in our model are complementary in that they explain the influence factors outside the scope of the other.

Deterrence theory explains individuals’ decisions to commit crimes as utilitarian calculations, based on benefits of performing the crime (utility) and punishments or sanctions for the crime (disutility). Although commonly applied to explain criminal behavior, Akers and Sellers observed that criminological theories explain law-breaking or “any deviant behavior that violates social norms, whether or not such behavior also violates the law” [1, p. 2], and is thus applicable to violations that may not be perceived to be criminal per se, but are still violations of law or at least social norms, such as software piracy. In essence, an individual will commit a crime if the expected benefits outweigh the expected costs.

Conventionally, most forms of deterrence theory-based models include severity and certainty of formal sanctions. More recently, less tangible forms of sanctions, such as shame [35]. Paternoster and
Simpson in their model also include moral beliefs about an act [34]. We include each of these concepts in our model. The effects of each of these constructs on software piracy are described below.

2.2.1 Formal Sanctions. Formal sanctions are explicit penalties imposed for specific forms of misconduct. According to Deterrence Theory, undesirable behaviors can be deterred by imposing formal sanctions. The more forceful or effective the sanction, the more undesirable behaviors will be deterred. Further, severity and certainty are important factors that determine the effectiveness of a sanction. Straub’s [45] research into computer abuse found that sanctions deterred users from committing computer abuse. D’Arcy [13] similarly found that the severity of formal sanctions had a significant effect on users’ intentions to commit computer abuses. Given this theoretical and empirical support, we hypothesize the following:

H8: Formal sanctions negatively affect intention to commit software piracy.

2.2.2 Shame. Following Braithwaite [6] and Paternoster and Simpson [34], we have included shame as a deterrent in addition to formal sanctions. Shame refers to a feeling of guilt or embarrassment if others knew of one’s socially undesirable actions [14, 35]. Tangney [49] held that shame affects an individual’s self esteem. Following Paternoster and Simpson [34], shame can be regarded as a deterrent because it is assumed to have effects similar to other sanctions [6, 15]. This means that individuals may estimate probable shame, just as one might calculate other sanctions [52]. In fact, research on deterrence has found positive evidence that shame functions as a deterrent and decreases individuals' motivation to perform crimes [23, 31]. Thus, we hypothesize that:

H9: Shame negatively affects intention to commit software piracy.

2.2.3 Moral Beliefs. It has been criticized that traditional views of deterrence do not take into account the moral beliefs of individuals [2]. These commentators maintain that offenders may refrain from offending, not because they fear sanctions, but simply because they evaluate the offense as morally wrong. Subsequent models of deterrence have incorporated moral beliefs [35]. Interestingly, Paternoster and Simpson [35] note that moral inhibitions were found to be the strongest predictor of corporate crime. This finding with respect to moral inhibitions is supported by various studies [2, 15]. For example, Bachman et al. [2] found that sexual assault was inhibited not only by formal sanctions, but also by the perceived immorality of the act. In fact, Bachman et al. [2] reported that formal sanctions were irrelevant for offenses regarded as morally wrong. Thus, we can hypothesize:

H10: Moral beliefs negatively affect intention to commit software piracy.

3. Methodology

3.1 Scenario Method

To empirically examine IS security policy violations, we employed a hypothetical scenario method, which poses respondents with a hypothetical situation followed by a question asking whether they would behave in the same way under similar circumstances [3, 13, 25]. This method choice was made for several reasons. First, software piracy, like other socially undesirable behavior, is difficult to measure directly via conventional means due to respondents’ tendency to conceal information or to respond to questions in socially desirable ways [53]. In contrast, because of the hypothetical, third-person nature of the scenarios, the scenario method provides an indirect means of measuring socially undesirable behavior, offering respondents a less intimidating means of reporting their intentions [25]. For this reason, the scenario method is commonly used to research ethical/unethical behavior in the social sciences [33]. A sample scenario used is shown below:

Brandon is considering downloading an unauthorized copy of an inexpensive image editing program. The software is developed by a modestly successful, foreign software company, which is currently the market leader. Brandon mainly makes unauthorized copies of computer games, but also copies software programs, just to see if he likes them. Brandon, who doesn’t have a lot of money, likes to try out software before buying it. However, Brandon has never paid for software. The software user manual states that making unauthorized copies is prohibited. Brandon decides to copy the software.

3.2 Instrumentation

Items were drawn from previously validated instruments where possible [46]. In cases where previous instruments used only a single indicator for an independent variable, additional items were derived to enable reliability testing. A preliminary version of the instrument was pretested to ensure measurement validity.
For the deterrence constructs, each severity of sanction measure was multiplied by its corresponding certainty of sanction measure. This yielded several composite sanction measures that “reflected both the risk and cost of perceived punishment” [31, p. 481].

The dependent variable, intention to software piracy, was measured using a single item: “What is the chance that you would do what [the scenario character] did in the described scenario?” The response scale ranged from 0 (“no chance at all”) to 10 (“100 percent chance”). Although Cook and Campbell [12] caution against the use of single-item measures to avoid monomethod bias that could prevent constructs from being reliably measured, Straub et al. [47] point out that in certain cases a single-item measure is most appropriate. Such is the case with the intention measure in scenario-based surveys in which the respondent is asked his/her probability of behaving similarly to the character in the scenario [38]. Because measurement error is not expected for this item, a single-item is typically used [35].

3.3 Data Collection

Data were collected from 183 undergraduate students at a large European business school. This sample was selected because students are a key demographic for software piracy [30]. The required sample size to evaluate our model is 100 according to the “rule of ten” heuristic [4]. However, we collected nearly double this number to ensure sufficient power and reliability in the results.

3.4 Model Validation

To establish factorial validity and reliability for our model, we followed the PLS validation procedures outlined by Gefen and Straub [19]. To test convergent validity, we performed a bootstrap with 500 resamples and then examined the t-values of the outer model loadings. Convergent validity is demonstrated when all indicators load significantly on their respective latent construct. In our case, all indicators exhibited loadings that were significant at the .001 level (excluded for brevity), denoting strong convergent validity.

To evaluate discriminant validity, two tests were performed. First, the cross-loadings of measurement items on latent constructs were examined. In this test, discriminant validity is demonstrated when an item more highly loads on its intended construct than on any other construct. Following Gefen and Straub [19], this difference in loadings should be at least .10. In this test, all items showed excellent discriminant validity (excluded for brevity). Therefore, the model demonstrates high discriminant validity.

A second test of discriminant validity is to compare the AVE score for each construct. In the AVE test of discriminant validity, the square root of a given construct’s AVE should be larger than any correlation of the given construct with any other construct in the model [9]. All the results of this test demonstrate strong discriminant validity. Finally, to test the reliability of measurement items, SmartPLS was used to compute the composite reliability score which is evaluated in the same way as Cronbach’s α [17]. These results exhibited a reliability score well over the .60 threshold accorded to exploratory research [32]. These statistics are reported in Table 1.

4. Results

We analyzed our model using Partial Least Squares (PLS) using SmartPLS software [40]. We chose PLS because of its usefulness in exploratory theory-building research and its ability to simultaneously evaluate the measurement and structural models [20, 10].
In testing our hypotheses, we controlled for the effects of two variables. First, because each respondent received one of four different scenarios, we controlled for the effect of the type of scenario received on the dependent variable. Second, we found that the reported realism of the scenario (e.g. “How believable do you think the above scenario is?”) correlated significantly with reported intention to commit software piracy ($r = .251$, $p < .01$). We therefore also controlled for the effect of perceived realism. In model analysis, only realism had a significant effect (path coefficient .14, $p < .05$).

### 4.1 Results of Theoretical Model Testing

The results of our theoretical model testing are depicted in Figure 2. Because of the directional nature of each hypothesis, one-tailed tests were used to assess significance.

Of the hypothesized neutralization techniques, condemning the condemners (.20; $p < .01$) and appeal to higher loyalties were significant (.19; $p < .10$). Both had a strong positive effect on intention to commit software piracy. However, the effects of the remaining neutralization techniques were not significant. Thus, hypotheses H1 through H7, only H1 and H4 were supported.

For the first two deterrence hypotheses involving sanctions, formal sanctions had no significant effect on intention to commit software piracy. Thus, H8 was not supported. The effect of shame, however, was significant (−.21, $p < .001$). Therefore, H9 was supported.

Finally, we hypothesized that moral beliefs would also influence intentions to commit software piracy (H10). We found that moral beliefs had a significant negative effect on intention, with a path coefficient of −.16 (p < .001). Thus, H10 was supported.

### 5. Discussion

Based on our empirical results we next highlight six findings. First and foremost, the neutralization technique appeal to higher loyalties significantly increases one’s intention to copy software. As mentioned, this is a new finding in the sense that previous research has not explicitly studied the effect of each neutralization technique in the copying of software [30].

Second, the neutralization technique, condemning the condemners, significantly increases intention to pirate software. As mentioned, this is a new finding in the sense that previous research has not explicitly studied the effect of each neutralization technique in the copying of software [30].

Third, the other components of the neutralization theory (denial of responsibility, denial of injury, the
Fifth, formal sanctions had no effect on corporate software piracy intention. This findings is different than previous results in software copying suggests. Higgins et al. [26] found that certainty of sanctions had an effect on an individual’s software copying, while severity was insignificant in reducing software piracy among home users.

Also previous findings regarding software copying by Peace et al. [36] suggests that formal sanctions have direct effects on the users’ attitude toward software copying. Nevertheless, our results are consistent with results in the area of corporate crime [37]. In the IS domain, D’Arcy et al. [13] also noted that the relationship between certainty of formal sanctions and intention to commit computer abuse was not significant, while severity of sanctions had a strong effect on intention to copy software. We have two explanations as why our results regarding formal sanctions differ from the previous studies on that area. First one relates the strong effect on neutralization as predictor of corporate software copying. Keeping this in mind, it could be that the users are under a spell of neutralization techniques, and as a result, see that they have rational reasons to copy corporate software in our hypothetical cases. Following this line of thinking, we may postulate that those users who justify their behavior through neutralization, may consider that they have not done anything that is punishable (hence, deterrence does not work). Second, deterrence theory asserts that if the likelihood of being caught and the severity of punishment are high, then an individual will be deterred. Perhaps the weak effect of formal sanctions on the intention to commit software piracy, is another explanation for our results. Even if an individual is caught then it appears the severity of punishment is also perceived as minimal.

Sixth, the effect of shame on intention to commit copying was significant. This finding is consistent with previous studies [26].

5.1 Limitations

This study is subject to typical limitations. Typical limitation stems from the use of intention as the dependent variable. As a result, a critical reader may ask whether intention indicates actual behavior. Two justifications are available from the literature supporting the use of intention as the dependent variable. First, measures of intention in criminological research are indicative of a motivation state or predisposition to commit an act [35] and are widely accepted in criminological research [8, 2]. Second, studies exploring the relationship between actual behavior and intention report a strong relationship between the two components [16, 24, 38]. So, while the fact that we did not measure actual behavior is a limitation, the use of scenario-based intention measure is an important approximation, and offers new insights for measuring software copying.

5.2 Implications for Practice

Based on our empirical findings, we offer a number of implications for software development companies, educators, and anti-piracy organizations. Our results suggest that those software development organizations, educators at different institutions and anti-piracy organizations that want to overcome software copying should focus on three aspects. First, is overcoming the justifications based on condemnation of the condemners and appeal to higher loyalties. Second is ensuring that people perceive the copying of software as morally wrong. A third aspect is shame, meaning that shame works as a potential deterrent.

In order to address the neutralization technique of appeals to higher loyalties, educators and anti-piracy organizations must make a convincing case that arguments such as it is acceptable to copy for a friend or someone who does not have money, are not tenable.

Regarding moral belief, the educators and anti-piracy organizations need to make a justified and convincing case that copying of software may not be morally acceptable. In order to do that, educators and anti-piracy organization could base their strategy on theories of moral thinking. The leading theory of moral decisions-making is that of Cognitive Moral Development by Kohlberg [27]. Kohlberg [27] suggested that individuals’ moral decisions-making encompasses six stages [42]. Of these, stage one is about sanctions and stage four is “it is wrong, because it is the law” stage. These lower stages are deemed irrelevant here, because the formal sanctions were insignificant in our sample, and the respondents in our scenario already realize that the action is illegal, rendering the “it is legal” argument irrelevant. Keeping these in mind, the stages that remain are second (“egoistic, own interest”), third
neutralization techniques. In this instance, we suggest the ability of persuasive discussion to “de-neutralize” the use of a pre- and posttest survey method. With this technique, researchers first obtain a baseline response. Then a carefully designed campaign or educational intervention is administered to employees. After this intervention, the effect of the intervention can be studied via the post measures. For the data collection, both subjective (interview, survey) and objective measures can be used.

While a number of studies have explored illegal copying of software by an individual (i.e., non-corporate context) from various theoretical viewpoints, the role of neutralization techniques has not been studied in the domain of corporate copying. Hence, one further area for future research therefore involves the application of neutralization techniques to corporate software piracy.

6. Conclusion

Illegal copying of software continues to be a major economic concern for organizations that both produce and use software. Given the widespread nature of the problem and the potential economical losses, the illegal copying of software has received considerable attention by IS scholars. Previous research indicates that neutralization – a form of rationalization by an individual – can help to explain software piracy intention. However, previous research does not indicate which techniques of neutralization contribute most to software piracy intention. Without this information, it is difficult to design the necessary campaigns and education interventions, aimed at overcoming these neutralization techniques. To address this gap in the research, we advance a model which encompasses the relationship between each element of deterrence theory and intention to copy software. Formal sanctions, shame and moral belief were also added to the model. The model was validated by students (n =183). Results show that appealing to higher loyalties and condemnation of the condemners strongly predicts intentions to copy software. In addition, shame and moral beliefs were also strong predictors. These findings have important strategic implications for anti-piracy organizations and scholars. For anti-piracy organizations, our results imply that these organizations should design different campaigns and education interventions aimed at overcoming two neutralization techniques (appeal to higher loyalties, condemnation of the condemners), and use moral education. In turn, the investment for formal sanctions should be carefully thought through.

For future research, it is suggested the effect of different interventions (e.g., campaigns and education) to overcome these two different neutralization
techniques should be studied. In addition, future research is needed to explore how such intervention efforts can be utilized while taking into account the fact that our respondents’ intentions to copy software were influenced by moral belief.

7. References