What Motivates Software Crackers?

Sigi Goode
Sam Cruise

ABSTRACT. Software piracy is a serious problem in the software industry. Software authors and publishing companies lose revenue when pirated software rather than legally purchased software is used. Policy developers are forced to invest time and money into restricting software piracy. Much of the published research literature focuses on software piracy by end–users. However, end–users are only able to copy software once the copy protection has been removed by a 'cracker'. This research aims to explore why, if copy protection is so difficult to remove, do crackers invest their skill and time in this activity instead of more lucrative and legal employment. This study develops a framework of neutralisation, justification and motivation and goes directly to the initial software crackers to determine what motivates their activities. The study first applies this framework in an anonymous online survey of crackers. The study then conducts cognitive interviews with eight crackers to explore and further validate the survey's findings. The study finds the challenge of removing the copy protection from software as the strongest motivation for the actions of crackers. Desire for social participation, while found to be rewarding, was considered unnecessary for crackers to continue their actions. Higher social status was not a motivational factor but was a perceived by-product of cracking. The study also raises areas for future research.

KEY WORDS: software piracy, personal motivation, social justification, neutralisation

Dr. Sigi Goode is a senior lecturer in Information Systems at the Australian National University, Canberra and a director of the Australian National Centre for Information Systems Research (NCISR). His PhD thesis dealt with construct validity in IS research. Dr. Goode has published in a variety of journals, including Information & Management, Journal of Global Information Technology Management, Journal of Computer Information Systems, Information Systems Management, Information Technology and Management and the Australian Journal of Information Systems, among others. His research interests include system adoption, mobile commerce, software piracy and open source software.

Mr. Sam Cruise has a First Class Honours degree in Information Systems from the Australian National University. Sam has also worked as a project officer for an IT and health research project and recently completed a Graduate Diploma in Education from the University of Western Australia. Sam is currently studying medicine at Griffith University. Sam's research interests include software piracy and policy, education and information systems use.

Introduction

Software, as a digital good, is expensive to produce but inexpensive to duplicate and distribute (Gopal and Sanders 2000). Because of the ease of duplication, it is in the software producers' interests to make it as difficult as possible to obtain illegal copies of copyrighted software (Maude and Maude, 1984). The literature indicates that firms spend substantial resources developing methods to prevent unauthorised duplication (Rosenberg, 1989; Schildkraut and Gasper, 2000; Wallach, 2001; Lee et al., 2002; Lee and Chen, 2002; Moore 2003).

Despite the efforts of software publishers, most of the devices used to prevent unauthorised copying and installation of software have been circumvented with sufficient skill and time. In 1984, Laind Huntsman, the head of software development for Formaster, a company dedicated to software protection, stated that "no protection system has remained uncracked by enterprising programmers for more than a few months" (Tyler, 1984). Martel Firing, the founder of Noumenon (a software publisher), stated "nobody has a total solution. We're just trying to defeat the casual copier" (Tyler, 1984). Wallach (2001) argues, "those determined to bypass copy-protection have always found ways to do so – and always will".

The role of the "cracker" in the distribution of illegal software is pivotal, since software cannot be illegally copied or used while copy protection is in place. Removing copy protection is difficult and time-consuming, as the cracker has to circumvent, usually without the benefits of seeing the program source code, the devices developed by paid software authors. This activity requires specialised technical skills, which could arguably be put to more legitimate use elsewhere. Additionally, evidence from the popular media suggests that crackers are not paid for their work (Piazza, 2002). Crackers also violate software copyright legislation and software licenses (Cambanis, 2002; Lee, 2002).

This study is motivated by two factors. First, the business PC application software industry accounted for worldwide revenues of US$21.6 billion in 1999 (Software & Information Industry Association 2000), a 19% increase from 1998. In 1999, the estimated losses due to software piracy were US$12.2 billion worldwide in the business software sector alone, an 11% increase from the previous year. The use of pirated software increased 34% from the previous year (Software & Information Industry Association 2000). Clearly, substantial funds are at stake.

Further, software authors must devise more complex means of protecting their software including expensive litigation processes (Hiduja, 2003) and copyright policy enforcement (Kini et al., 2000). Managers suffer losses as fewer units of software are sold and policy developers must spend resources trying to stop the supply and use of pirated software (Gopal and Sanders, 2000; Moores and Dhaliwal, 2004).

Second, there has been much research into why end-users use pirated software (Davis, 1989; Eining and Christensen, 1991; Shim and Taylor, 1991; Logsdon et al., 1994; Simpson et al., 1994; Givon et al., 1995; Sims et al., 1996; Gopal and Sanders, 1997; Gopal and Sanders, 1998; Limayem et al., 1999; Rahim et al., 1999). Most studies in the area have used student samples, ostensibly for convenience and access purposes (Kwong et al., 2003). However, there has been seemingly little attempt to understand the motivations of the individuals who *initiate* the spread of this software. The dearth of literature in this area makes for a particularly intriguing study, and this paper answers the call of authors such as Hinduja (2003), Sims et al. (1996) and Glass and Wood (1996), among others.

This discussion suggests two main research questions. The apparently time-consuming and difficult tasks performed by the cracker raise the question of what motivates a cracker.

1. What factors motivate software crackers to remove copy protection from commercial software?

This study also aims to explore how individuals neutralise the social controls that would otherwise inhibit deviant motivational patterns (Sykes and Matza, 1957). This study includes neutralisation (justification) as part of a general theory of motivation (Minor, 1981).

2. What factors do software crackers use to justify removing the copy protection from commercial software?

The rest of this paper is structured as follows. The next section discusses the software piracy literature. This is followed by the theoretical framework, which comprises research literature on motivation and justification, producing factors to proxy for both personality aspects. The paper then details the research method, including the survey instrument and cognitive interview method. The paper then discusses the results and analysis, including quantitative and qualitative analysis of the survey results, and the exploration of these results using interviews. Finally, conclusions, implications and areas for further research are covered.

Software cracking and software piracy

Software piracy is defined as "*the unauthorized copying of computer software, which constitutes copyright infringement, for either commercial or personal use*" (Software & Information Industry Association 2000). Wold and Shriver (1989) were among the first to document the rise of piracy, which increased as computers became more widespread. Figure 1 describes the software piracy process.

Figure 1 illustrates the pivotal role that crackers play in the distribution of pirated software. First, suppliers provide the group with software, which may originate from software authoring firms, reviewers or retailers. Crackers, who have the most technologically complex role, strip the programs of their copy protection - the control techniques used
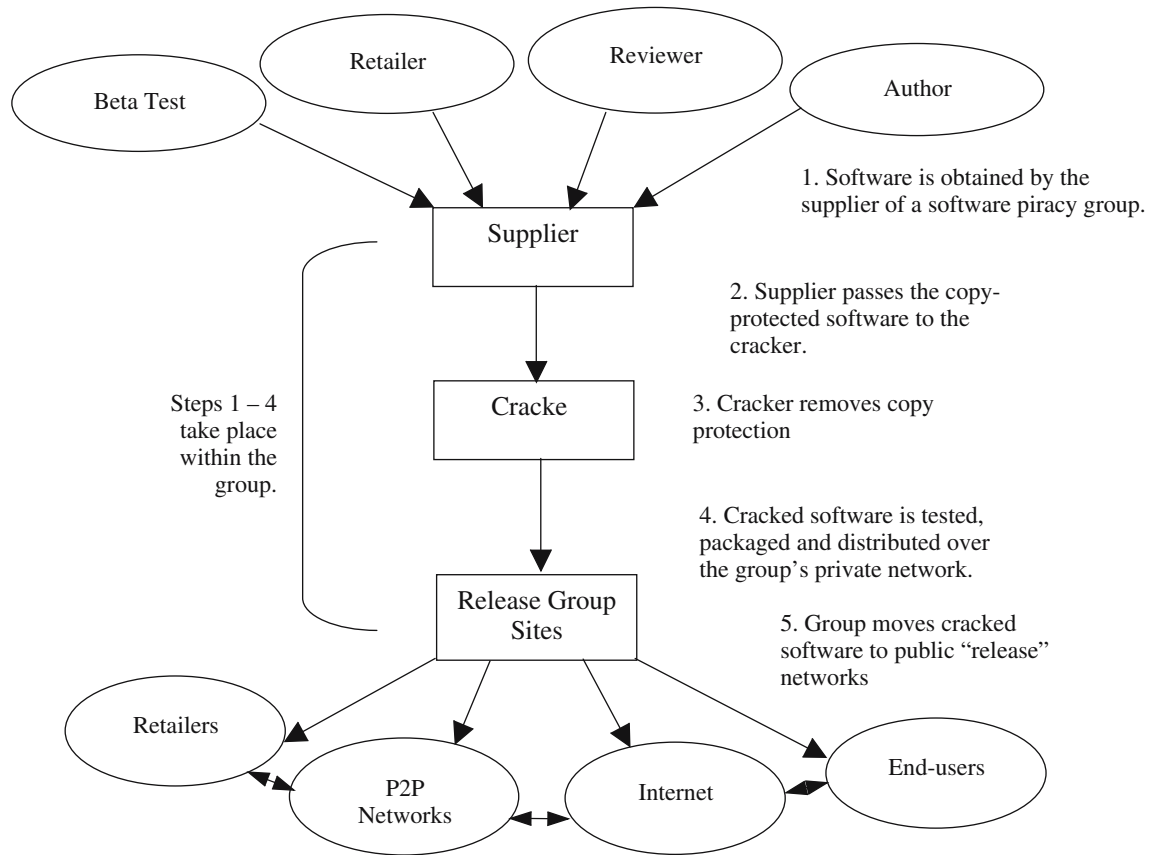
Figure 1. The pirated software distribution process.

to prevent unauthorised duplication (Maude and Maude, 1984). Testers then ensure that the software works properly by conducting test installations on different computers. Packers divide the programs into small files and distribute them to release sites. Finally, Pre-releasers use File Transfer Protocol (FTP) programs to move the files to the group's 'release site' (Lee, 2002). From this point, external courier groups take over and move the files through a systematic distribution chain, and eventually into Usenet newsgroups, peer-to-peer software networks (Lee, 2002) and pirate software retailers (Moores and Dhillon, 2000).

Published research has generally focused on end-user piracy. Recent studies have found that gender and age affect piracy behaviour, with females and older individuals less likely to use pirated software (Solomon and O'Brien, 1991; Simpson et al., 1994; Gopal and Sanders, 1997). The literature profiles the typical computer criminal as young, skilled, knowledgeable, overqualified for their position, elitist, and

believing that their computer use did not harm anyone who could not afford or did not deserve to be harmed (Highland, 1984).

Several studies have found relationships between a formal code of ethics or behaviour, such as at a place of business, and an individual's decision to pirate software (Pierce and Henry, 1996; Gopal and Sanders, 1997; Al-Jabri and Abdul-Gader, 1997). Some have speculated about similar unwritten codes of behaviour within other subcultures, such as street gangs (Winchester and Costello 1995) and prison communities (Winfree et al., 1994). However, other codes, such as personal or informal codes, appear significantly less influential (Pierce and Henry, 1996). Limayem et al. (1999) found no significant difference in attitude towards software piracy between those who attended an ethics course and those who did not.

Situational events, such as inadequate time to acquire software or not knowing where to obtain the software legitimately, and personal gain factors

significantly affect an individual's decision to copy software (Simpson et al., 1994). This may be due to "deindividuation", the feeling of anonymity and distance from the adverse effects of the person's actions (Loch and Conger, 1996).

Software crackers may feel as though they are aiding others by providing free software, consistent with Glass and Wood (1996) and evidence from Constant et al. (1996) of altruism in helping strangers over the Internet. There is evidence in the popular media that group members earn no money from piracy (Cambanis 2002; Mackenzie 2002) instead describing the activity as a social experience which was motivated by a sense of competition, prestige, and the entertainment value of distributing pirated goods (Lee, 2002).

Theoretical framework

This study divides its theoretical framework into two arms. The study draws first on theories of motivation and, second, on theories of justification and social neutralisation.

Theories of motivation

Motives are regarded as the basic causes and determinants of all behaviour which is not haphazard, trivial, or purely habitual, and is divided into two broad categories (Ford, 1992). The first type of motivated behaviour involves behaviour in which the individual feels forced, perhaps against their will, to act in certain ways (for instance, to seek food). The other type describes behaviour in which the individual is clearly conscious of a definite goal to which they are persistently and forcefully directed (Vernon, 1969). This includes consequences that the individual would like to achieve (Ford, 1992). This study considers the second type of motivation.

Motivation can be externally based when the individual seeks affirmation of personal values (Barnard, 1938). Individuals may aim to gain group acceptance (Katz and Kahn, 1966) and, subsequently, to gain status (Etzioni, 1961; Barbuto and Scholl, 1998). In addition, the individual sets internal standards of values that become the basis for the 'ideal' self (Barbuto and Scholl, 1998). Other studies

addressing this 'actualization' (Maslow, 1943) describe the need for achievement (McClelland, 1961) and growth associated with developing one's potential (Alderfer, 1969). Hence, the challenge of cracking may itself be a significant motivating factor.

There may also be intrinsic motivation (Barbuto and Scholl, 1998) where the activity itself is the incentive (Deci, 1975). Intrinsically motivated behaviour is of two kinds. First, an individual may seek to behave in ways which allow them to feel competent and self-determining (Deci, 1975). The second kind of intrinsically motivated behaviour involves conquering challenges. When an individual conquers the challenges that they encounter, they will feel achievement (Deci, 1975). There is evidence that the greater the difficulty of the challenge, the greater the motivation to succeed in the challenge (Locke, 1968). The knowledge gained from undertaking the challenge may itself be rewarding and hence motivating to an individual. Maslow (1943) postulated that there was "a basic desire to know, to be aware of reality, to get the facts, to satisfy curiosity".

Finally, while anecdotal evidence has suggested that crackers are not paid for their activities (Lee, 2002), there is no conclusive proof that this is the case. Instrumental rewards such as salary or bonuses may motivate individuals when they perceive that their behaviour will lead to tangible benefits (Barnard, 1938; Katz and Kahn, 1966). This is similar to the need for power (McClelland, 1961), a need for safety (Maslow, 1943) or the later stages of existence needs (Alderfer, 1969). Instrumental reward cannot therefore be excluded as a possible component of cracking motivation.

Factors of motivation

Figure 2 describes the application of motivation factors extracted from the literature review to the study of software crackers.

Theories of justification

When behaviour exhibits signs of deviance, it is necessary to understand how the individual neutralised the social controls that would otherwise check or inhibit deviant patterns (Sykes and Matza, 1957).

Factor	Description
Desire for Social Participation	Crackers may find the social participation of the piracy environment to be highly rewarding (Lee 2002). Individuals may have a need to interact socially (Maslow 1943) or be part of a group (Katz and Kahn 1966, Turner 1984, Ashforth and Mael 1989).
Desire for Personal Challenge	If removing copy protection is extremely difficult, then the challenge itself may be a significant motivating factor for crackers (Locke 1968, Deci 1975), consistent with the related psychological theories (Lee 2002).
Desire for Social Status	The competition between groups (Lee 2002) and the behaviour of individuals inside groups to seek status (Etzioni 1961, Barbuto and Scholl 1998) suggests that this may be a motivating factor.
Tangible Reward	Individuals may feel motivated when they perceive their behaviour will lead to extrinsic tangible outcomes such as pay or bonuses (Barnard 1938, Katz and Kahn 1966). It is anticipated that this factor of motivation will act solely as a control in the light of evidence that that crackers are not paid (Lee 2002).
Public Demand for Free Software	Altruism may increase the likelihood of people providing software for illegal copying (Glass and Wood 1996). There is further support for the provision of assistance to strangers for no tangible reward (Constant *et al.* 1996).
Personal Need for Free Software	Financial constraints can be a motivating factor for end-users to pirate software (Simpson *et al.* 1994, Glass and Wood 1996).

Figure 2. Factors of motivation in the context of software piracy.

Factor	Description
The Denial of Responsibility	If subjects deny responsibility for their actions, then the restraining effect on behaviour can be reduced. This denial of responsibility helps them renounce culpability for their deviance, instead perceiving themselves as victims of their environment (Sykes and Matza 1957).
The Denial of Injury	Subjects may deny that any injury or harm arises from their actions. This allows offenders to feel that their deviance may be undertaken without direct harm to others (Sykes and Matza 1957).
The Denial of the Victim	It is possible that, despite accepting responsibility for the deviant actions and resulting injury, the subject may justify the action as retribution upon or in the absence of a deserving victim (Sykes and Matza 1957).
Condemnation of the Condemners	The subject may attempt to transfer attention from their own deviant acts to those who disapprove of their actions. The subject may claim that the condemners are hypocrites, thus blaming their actions on law-makers or other officials (Sykes and Matza 1957).
The Appeal to Higher Loyalties	The subject justifies and legitimises their deviant behaviour by claiming that they are being loyal to an "unconventional social bond", which bears greater personal relevance (Sykes and Matza 1957).

Figure 3. Factors of justification in the context of software piracy.

The techniques of neutralisation (Sykes and Matza, 1957) are a popular means of exploring the justification of deviant behaviour, having been applied in fields as varied as adolescent drug use (Peretti–Watel, 2003), the behaviour of beauty pageant mothers (Heltsley and Calhoun, 2003), and deer poaching (Eliason and Dodder, 2000). Further, past research has found that the techniques of neutralisation are

particularly valuable in white collar crime (De Young, 1988; Hollinger, 1991; Strutton et al., 1994; Dabney, 1995; Gauthier, 2001). Lim (2002) examined the role that neutralization played in cyberloafing, where employees use their company's Internet access for personal purposes during work hours.

Factors of justification

Sykes and Matza (1957) identify the factors of justification and neutralisation shown in Figure 3.

Research method

Because the target population is likely to be somewhat specialised, anonymous and risk-averse, there was significant concern that it may be difficult to find participants. Indeed, this is the case for much 'sensitive research' which examines controversial or personal issues (Lee, 1993). Sieber and Stanley (1988:49) also observe the adverse effects of "potential consequences or implications...for the participants in the research or for the class of individuals represented by the research". Despite this, "the more promising areas of business ethics research are 'sensitive'" (Dalton et al., 1997:1049).

At the same time, validity is important to research in areas such as ethics and social behaviour. Many social scientists consider validity to be one of the most important aspects of social science research (London, 1975; Anastasi, 1982), however it is especially important when few observations are available. By increasing the number of observations or participants in a study, the researcher can be more certain that the research is actually "measuring what it purports to measure" (London, 1975).

Amid the research methods available to the social science researcher, such as case studies (Klein and Myers, 1999), experiments (Mason, 1989), surveys (Davis, 1989), and action research (Lau, 1997) the survey method has been shown to be an effective means of gathering data electronically. It has also received substantial literature attention (Joinson, 1999; Simsek and Veiga, 2000; Cheyne and Ritter, 2001; Simsek and Veiga, 2001; Nosek et al., 2002). The method has proven useful in the early stages of

research (Dubin, 1978; Malhotra and Grover, 1998). The advantage of the survey method is that a range of variables can be examined *in situ* with little time (Dubin, 1978; Malhotra and Grover, 1998).

However, the survey method only portrays the state of affairs at a single point in time, provides little insight into causal relationships, and is open to respondent and researcher bias (Galliers, 1992). Dalton et al. (1997) argue that these drawbacks can be magnified when the research is of a sensitive nature. The immediacy and effectiveness of the survey method was thought to outweigh these potential disadvantages. As a result, it was acknowledged that a survey should be complemented by a substantive interview approach in order to explore the findings in detail. A key methodological goal of this study is not simply the qualitative confirmation of quantitative findings, but also the triangulation of findings (consistent with Deacon et al., 1998).

Accordingly, this study takes a two-stage approach to data gathering and analysis. The first phase of the study uses a questionnaire survey to examine attitudinal items. The second phase uses cognitive interviews to triangulate and add validity to the findings, by exploring the survey outcomes in greater depth.

Phase 1: Questionnaire survey

An online electronic survey was deemed the most suitable research approach for the first phase. While respondents must be carefully and appropriately targeted in order to produce good results (Cheyne and Ritter, 2001), individuals may also exhibit lower social desirability when they respond to online surveys compared to paper-based surveys (Sproull and Kiesler, 1991; Joinson, 1999; Cheyne and Ritter, 2001; Lim, 2002).

Population definition and sample selection
As the actual size of the cracker population could not be found in the published literature, the survey phase of this study used a sample of the population (Adams and Schvaneveldt, 1991). Three methods were proposed as means of soliciting participants. These included scanning pirate group contact documents for email addresses, soliciting participation in online

real-time chat forums and soliciting participation in online message boards.

Method pre-testing suggested that soliciting participants on online message boards was the most viable choice. This technique has been used previously (Cheyne and Ritter, 2001; Lim, 2002) and is considered a suitable means of soliciting participants. This technique allowed appropriate potential respondents to be targeted (Cheyne and Ritter, 2001). Also, this type of participant recruiting is particularly useful when the researcher requires control over who hears about the study and how the study is described (Nosek et al., 2002).

Survey development

Straub (1989) argues that poorly-constructed surveys can compromise otherwise sound research. Issues such as length, appearance and number and type of questions are fundamental to survey validity. Survey structure was important as data had to be gathered from a variety of individuals with unknown demographics.

The survey first examined the eleven factors of motivation and justification using a series of Likert-scale questions. Where possible, questions were adopted from existing instruments in the literature that had already undergone testing (such as Solomon and O'Brien, 1991). However, the exploratory nature of this research meant that existing questions for some factors could not be found, and new questions had to be developed. These new questions were subjected to extensive pre-testing. Each of the eleven factors of motivation and justification was mapped to one or more questions in the instrument. Questions used a seven point Likert scale to determine respondent attitudes (Likert, 1932).

The survey also contained a series of open-ended questions, designed to explore the factors of motivation and justification in greater depth. The open ended questions would give the respondent the opportunity to explain their answers to the Likert-scale questions. Again, questions were adapted from the literature, where possible, such as Sykes and Matza (1957).

Demographic information was also collected at the conclusion of the survey. The survey had to be anonymous as the identity of an individual could not be ethically solicited in circumstances where they may admit to criminal activity. Demographic data were collected only in relation to age, education level reached, current area of employment, and whether or not the respondent is still active in the piracy environment. This demographic data has been deemed the most significant in past studies involving online subculture deviance (Highland, 1984). Demographic questions were optional so as to allay fears about data misuse and hopefully increase response rates (Kotulic and Clark, 2004).

Pre-testing is deemed important as it allows the researchers to examine the usability and fluidity of the survey (Dillman, 1978; Grover et al., 1994). The survey was tested on two crackers, known personally to the researchers. Problems with grammar and structure were addressed. A final version of the survey instrument was created based on the results of this pilot test.

Survey administration

Before administering the survey, a list of potential respondent questions and appropriate answers was produced so that each respondent would receive the same information about the study (Dillman, 1978). These included information regarding the aims of this research and the identity of the researcher (consistent with Kotulic and Clark, 2004).

In order to limit problems such as subjects forwarding the survey to others (Simsek and Veiga, 2001) and multiple responses from a single individual (Smith and Leigh, 1997), participants were solicited by way of an advertisement at five known cracking forums (Simsek and Veiga, 2001). Participants responded to an email address and were then issued a survey, which was accessible as a text document, as an attachment to the email, or by a hyperlink to a web-based survey. The web-based survey was only accessible by using the one-off password contained within the email.

Phase 2: Cognitive interviews

The second phase of the research method aimed, if possible, to gain additional insight into the findings from the previous stage. To do this, a method of cognitive interviewing was used. The interview method allows for the qualitative exploration of

important points on a personal level and gives flexibility in terms of research approach (Creswell, 1998). Friedman (1997) used a similar approach to explore the adolescent understanding of piracy and ownership beliefs.

Each interview followed the general program of cognitive interviewing outlined by Waldron (1986) and Scott et al. (1991). First, summary data were gathered and presented to the participants. The actual question was read to the interviewee. If the interviewee so desired, the question was repeated for clarity. Each finding was then related to the interviewee in terms of the information sought. The interviewee was then directed to confirm their understanding of the question and its meaning. The interviewee's open-ended reactions to both the question and the finding were then recorded for further analysis.

In order to obtain participants for this stage, calls for additional interviewee participants were posted on two cracking forums. It was hoped that some prior participants might direct others to participate

and lend credence to the study. Potential participants were given the choice between a telephone interview, an online interview using IRC (Internet Relay Chat) or a text-based interview using Private Messaging on discussion forums. All participants preferred the online interview option.

Results and analysis

Phase 1: Questionnaire survey

A total of 28 people replied to the posts in the cracking forums to express an interest in participating in the survey. From these, 26 responses to the survey were received. Of these, two were judged to be overtly hostile or incomplete, leaving 24 usable responses. Surveys were judged incomplete if they contained more than five unanswered questions. Table I shows the demographic statistics. Four of the 24 respondents declined to provide demographic information.

TABLE I

Survey participant demographics

Demographic	Category	Frequency
Age[†]	16–20	7
	21–25	5
	26–30	4
	31–35	1
	36–40	0
	41–45	0
	45–50	1
Area of employment	Unemployed	4
	Student	4
	Hospitality	3
	Information Technology	6
	Media	1
	Agriculture	1
	Self-Employed	1
Level of education[††]	Currently at High School (Years 7–12)	4
	Completed High School	3
	Attending University	4
	Completed University (Bachelor Degree)	5
	Graduate Degree (Masters or Higher National Diploma)	4

[†] Two respondents answered in terms of bandings. These responses are omitted from the above table.
[††] The Higher National Diploma, available in the USA, is a two year graduate degree with a prerequisite Bachelor degree.

Past studies of deviant electronic subcultures suggest that participants in these subcultures are young, skilled, and knowledgeable (Highland, 1984). The demographics support this: most of the respondents are 25 and under and have at least some degree of tertiary education. Seven had not attended University.

Tentatively, one surprising element in these demographics is the variation in areas of employment. Bearing the size of the respondent group in mind, only six of the 24 respondents work in the IT industry, contrary to a much higher IT industry employment rate predicted in other studies (Barber, 2001). The remainder of the respondents worked in fields as varied as agriculture or as a cook, with one respondent being self-employed and in turn employing five other people.

Analysis of motivation and justification

As observed in other studies of sensitive topics, the difficulty in finding respondents means that the sample size can be small. In circumstances where assumptions about the population cannot be made, perhaps due to the number of observations, nonparametric tests are appropriate (Anderson et al., 1987). The sign test was used to test that the median response was significantly different from the expected binomial median. Table II gives the median, mean, standard deviation and two-tailed p-values at the .05 level for the factors of motivation (Labovitz, 1970).

The results suggest that the *Demand for Free Software* and the *Desire for Social Participation* of cracking are rewarding, however they are not motivating factors. For the *Desire for Personal Challenge* factor group, the results strongly suggest (Median = 7, Sig. = .000 for both indicators) that crackers enjoy copy protection which is particularly difficult to remove and that the act of cracking software appears to be more important to the cracker than releasing the software publicly. The evidence suggests that crackers believe people should pay for software they use (Mean = 5.67, Sig. = .000) and that crackers do not limit themselves to cracking software that they personally need (Mean = 2.21, Sig. = .001). The *Desire for Social Status* did not appear to be a motivating factor in this analysis, though the results were unclear: crackers would continue their work anonymously if necessary (Mean = 6.63, Sig. = .000), however, the value of being recognised for cracking software was ambiguous (Mean = 3.17, Sig. = .075). Finally, *Tangible Reward* appeared to be insignificant as a motivating factor to crack software (Mean = 1.67, Sig. = .000).

Quantitative analysis of the factors of justification shown in Table III was less clear than the analysis of factors of motivation. This suggests that crackers may have individual ways of justifying their activity. With regard to the *Denial of Responsibility*, piracy countermeasures have little or no influence on a cracker's decision to crack software. The findings for the *Denial of Injury* factor were unclear, with crackers having varying views on the adverse effects of software cracking (Mean = 4.33, Sig. = .503). Based on the results for the *Condemnation of the Condemners* factor, it appears that crackers show some limited sympathy for the software industry (Mean = 4.92, Sig. = .031), however some also believe the industry does not deserve to have their product copied.

Phase 1B: Qualitative analysis

Open-ended questions were analysed using open coding. Open coding is the analytic process through which concepts are identified and their properties and dimensions are discovered in the data. This process involves creating a dictionary of key concepts from the central ideas mentioned in the responses by the crackers. From this dictionary, categories or concepts that stand for phenomena are created (Strauss and Corbin, 1998). The categories are presented, along with a count of the occurrences of a category's phenomena group responses. For each factor below, example textual passages are included to clarify scope and meaning. A participant's response may include entries in more than one category if multiple phenomena are evident in their response.

Desire for social participation

Table IV contains the open-ended questions and coded responses for the discussion on the desire for social participation within the context of software cracking.

Most crackers' relationships with other crackers extended beyond software piracy. Only a quarter of all survey respondents had even met members of their group in real life. Only five respondents

Sigi Goode and Sam Cruise

TABLE II

Factors of motivation

Factor	Indicator Question	Median	Mean	Std.Dev	Exact Sig.
Desire for social participation	The social aspects of the cracking scene are highly rewarding.	5	4.58	1.840	.263
	I would crack software even if it was not done in a group environment.	7	6.33	1.404	.000★
Desire for personal challenge	Even if I was not able to release the software I would still crack software just for the challenge it involves.	7	6.17	1.239	.000★
	Cracking a piece of software is more enjoyable if the copy protection is particularly difficult to remove.	7	6.46	1.414	.000★
Public demand for free software	The demand for free software is an important factor in my decision to continue cracking.	1	2.17	1.736	.000★
	People should pay for software that they use.	6	5.67	1.523	.000★
Personal need for free software	I only crack software that I need personally.	1.5	2.21	1.560	.001★
	I would pay for software when I could download a fully functional, cracked version for free.	4.00	3.75	2.289	1.000
Desire for social status	I would crack software even if I had to do it anonymously.	7	6.63	0.924	.000★
	Getting recognition for cracking software is important.	2.5	3.17	2.239	.075
Tangible reward	Tangible reward (monetary or otherwise) is the driving force behind my decision to crack software.	1	1.67	1.404	.000★

★ Significant at the .05 level.

reported that their communication with other group members was limited to software piracy.

Demand for free Software

Table V contains the coded responses to the open-ended questions on the demand for free software in the context of software cracking.

This anecdotal evidence suggests that crackers do not have a problem with having to pay for commercial software. However, there is significant support for the argument that the situation in which the software is purchased, and the quality of the software, should determine the cost of the software.

Desire for social status

Table VI contains the coded responses to the open-ended questions on the desire for social status in the context of software cracking.

While there is strong support for the proposition that crackers do indeed enjoy higher status (in differing degrees) in the Internet piracy environment, seven out of nine of the respondents who stated they were treated better because they were crackers continued on beyond the scope of the question to state that status was not needed for them to continue cracking software. This suggests that higher status is a by-product of cracking and not a motivational factor. Again there is a polarity in the responses for this question.

Desire for personal challenge

Table VII contains the coded responses to the open-ended questions about the desire for personal challenge in the context of software cracking.

The challenge of cracking is clearly a significant motivation for crackers to remove the copy pro-

TABLE III

Factors of justification

Factor	Indicator Question	Median	Mean	Std.Dev	Exact Sig.
The denial of responsibility	The disapproval of the commercial software industry has little or no influence on my decision to crack software.	6.5	5.62	1.837	.003★
	The disapproval of the law enforcement agencies has little or no influence on my decision to crack software.	6.5	5.46	2.146	.004★
	The actions of others forced me into cracking software.	1	2.46	2.146	.035★
The denial of injury	No-one is really hurt as a result of software piracy.	3	3.38	1.789	.041★
	Cracking software has a significant, adverse effect on the software industry.	5	4.33	1.810	.503
The denial of the victim	The software industry does not deserve to have its product illegally copied.	5	4.79	1.841	.064
	The software industry has no right to complain about the actions of software crackers.	3	3.25	1.894	.052
Condemnation of the Condemners	I hope that the software industry is not adversely affected by my actions.	5	4.92	2.020	.031★
	The software industry is a bunch of hypocrites who deserve everything they get.	4	3.29	1.756	.210
The appeal to higher loyalties	People that cannot afford a piece of software should not have access to it.	2.5	2.92	1.863	.078
	My actions as a software cracker constitute a service to the community at large.	4	3.54	2.226	1.000
	People should have to pay for software.	5	4.54	1.817	.238
	The benefits of my actions, as a software cracker, to the public justify the costs to the software developers.	4	4.00	1.865	.815

★ Significant at the .05 level.

tection from commercial software. The only responses that may undermine the inclusion of personal challenge as a motivational factor stated that, although the difficulty of cracking was initially a motivating factor, its effects were diminished as experience in programming increased. However, responses of this type were in the minority.

Personal need for free software
Table VIII contains the coded responses to the open-ended questions on the personal need for free software in the context of software cracking.

The responses to this question contain a great deal of variation that cannot be explained by demo-

graphics or group/scene affiliation. They are discussed in the following section.

Tangible benefits
Table IX contains the coded responses to the open-ended questions on the effect of tangible benefits in the context of software cracking.

There is strong support for the conclusion that tangible benefits do not influence the decision to crack software. Indeed, a significant proportion of respondents were openly hostile to the concept of people making money from cracking, perhaps providing evidence for the existence of a personal credo by which crackers operate.

TABLE IV

Desire for social participation

Code	Freq	Example
Stimulus: *Do you find the existence of competition between release groups a compelling reason to crack software?*		
Counter-Productive	7	"Cracking groups should work together"
		"Just cracking to get releases takes away the fun for me"
Competitive challenge	6	"It's always fun to race a big title and win. Gives you a feeling of 'we are the best'"
		"Competition makes you push hard, get faster and code more astonishing things"
Not part of a group	6	"I don't care about other groups or their individuals"
		"I try to stay away from release groups and things of that nature"
Promotes incompetence	2	"...promotes the release of nonworking cracks"
		"...can make less experienced group to release fast and not check the quality of their work"
Outgrow groups	2	"When you develop a serious interest in software reversing, groups become a drag and they restrict you from being able to share information"
		"It's always fun to release more then the other members, to make more keygens and be on the top of all the team stats"
Stimulus: *Does your relationship with other members of the group exist outside of software piracy? If so, in what capacity?*		
Discussion not limited to piracy	13	"It's impossible to talk with people only about software protections."
		"I have developed friendships with people I've met in the cracking scene that extend outside the realm of cracking software"
Close-friendship	7	"The people I met through cracking have become extremely close friends to me over the years"
		"Sure, in the 'scene' you can meet some really amazing people with equal interests"
Real-life social interaction	6	"[group name] have had cracking LAN's where we met each other and spent 3 days together"
		"I know many people from my own group, we met a few times together... drinking beer, vodka and etc"
Discussion limited to piracy	5	"I don't even know some of their real names, and we keep it that way"
		"No, for security reasons you have to be very discrete"
Constant communication	4	"I speak to [them] on irc or phone every day"
Interaction limited to internet communication	4	"I actually only have contact with other crackers and reversers though the internet"
		"Only in rare cases do real world relationships mean face to face meetings"

The denial of responsibility

Table X contains the coded responses to the open-ended questions for discussion of the denial of responsibility in the context of software cracking.

These responses indicate that crackers have entered into the decision to pirate software with full control over their actions. Only two respondents indicated there was a group of people that could influence their participation in software cracking.

A polarity in the responses is evident here, with almost half of the respondents stating the threat of punishment was ineffectual and the other half stating it had a significant effect. It is worth noting that most of the reasons why the threat of punishment was considered effective concerned the recent arrests of members of the Internet piracy environment, particularly the DrinkOrDie group.

The denial of injury

Table XI contains the coded responses to the open-ended questions on the denial of injury in the context of software cracking.

There is a polarisation of results in the responses to this question. Most respondents are able to recognise the damage caused to the software companies by their actions. Since they are not denying injury to their victims, some other technique of neutralisation is likely being used. However, there are clearly respondents who acknowledge their actions have some negative effects on the software industry, while there are others who even believe their actions are beneficial.

The denial of the victim

Table XII contains the coded responses to the open-ended questions on the denial of the victim in the context of software cracking.

Half of the responses indicate a lack of concern about the size of a software company when it comes to pirating its software. The other half use different reasons for considering the size of a software company. While eight responses indicate a wish to avoid harm to smaller software companies, the remaining four responses indicate that the respondents did not crack software from larger companies for fear of retribution.

TABLE V

Demand for free software

Code	Freq	Example
Stimulus: *Should all software be free? Please explain your answer.*		
Software need not be free	20	"No. Software developers must be supported through the purchase of software"
		"No. A professional has the right to ask for money in exchange of his job"
		"Of course not, development companies wouldn't be able to support themselves"
Software companies over-charge	10	"The big companies...charge way too much for their products, especially with an upgrade every 6 months or year"
		"I do think that much commercial software is ridiculously overpriced"
		"Some programmers produce absolute crap and expect 100's of dollars for it"
Only pay for worthy software	7	"I support software which I would like to use and think is reasonably price"
		"I use WinRar, mIRC and FlashFXP a lot, I will buy them all because I use them on a regular basis and the price is acceptable"
Poor should not be denied access	7	"When we look at expensive software, like $5000, lets say 3D Studio Max...NO ONE below the age 25 will ever have the money to pay for such a license, should that mean the person has to wait 10 years before he can start practise on 3D modelling?"
		"Software should be available to all, more so in developing countries where the cost of some software is the equivalent of a year or more's wages"
Donation-based software	2	"I believe that donation-based open source is the answer to this issue, for all digital medium (music, books, software)"
		"I often donate to authors who use a donation-based approach even if I don't use their software, just to support the effort"
All software should be free	1	"Sure, why not...very often share or trial versions are so restricted it's impossible to properly use and appraise it"

A total of five respondents believe that their actions can remedy bad corporate practices in software companies. The same number believe that the pricing of software has led to the proliferation of pirated software today. Six respondents believe that the actions of the software industry have no effect and the popularity of pirated software is explained by other factors.

The condemnation of the condemners
Table XIII contains the coded responses to the open-ended questions about the condemnation of the condemners in the context of software cracking.

There is evidence of the condemnation of the condemners in the responses to this question. Seven respondents believe that the commercial software industry reaction is incorrect while another 6 believe the industry reaction is futile and will have no effect on piracy. While there are responses supporting the actions of the industry, the examples quoted by the respondents indicate a support of the industry response in an area removed from Internet software piracy.

Six respondents accept the inevitability of law enforcement agency efforts to address software piracy. Further, these responses indicate an acceptance

TABLE VI

Desire for social status

Code	Freq	Example
Stimulus: *Do your actions as a cracker afford you a higher status on the Internet? If so in what capacity?*		
Afforded more respect	9	"I have a somewhat "high" status in a sense, as I am real popular amongst my fellow crackers"
Crackers are elite	7	"The groupie mentality kicks in and the people that DON'T know you treat you as a demi-god"
		"Sometimes when ppl come in to my channels on IRC, they talk to me like I am 'god all mighty'"
		"Yes. When you have a high status on the net, people know you. Admire you."
Status is unnecessary	7	"There is some respect for a crack but it's not a motivator"
		"It's rather fun to go onto IRC and have people message you with 'I'M YOUR BIGGEST FAN!' but I don't really use it as a motivation"
		"There is some respect for a crack but it's not a motivator"
Name is recognised	7	"My experience in the reverse engineering scene does give me the power of name recognition"
		"People in the scene recognize me but people don't come falling at my feet"
Access to restricted goods	5	"I can get some things which are, for others, not accessible"
		"You get access to non-public tutorials, tools, warez and so on"
Educator status	2	"The only 'higher' status I get is when I help someone who has less knowledge about cracking or reverse engineering"
		"If you have a lot knowledge then people look up to you to learn more things for themselves"
Stimulus: *Should other people be grateful to you for providing cracked software? Why / why not?*		
Gratitude does not matter	11	"I don't crack to make other people happy"
		"The last thing I care about while I'm cracking is the general public"
		"I do it for fun and for my own pleasure"
		"I crack software for fun mostly, not for people"
Gratitude is desired	9	"Yes they should...One minute and they have what they wanted. And who gave them these great services? The crackers"
		"Of course they should, many 'leechers' don't care about the time we spend on a protection"
		"I guess they should be grateful if I crack something they request"

that, as crackers, they are breaking the law. Five respondents have taken issue with the recent crackdown on release groups across the world. The example most often quoted was the arrest and prosecution of the DrinkOrDie members. Tellingly, while some respondents indicated that the actions of law enforcement were justified, none deemed their actions appropriate.

The appeal to higher loyalties

Table XIV contains the coded responses to the open-ended questions about the appeal to higher loyalties in the context of software cracking.

Non-respondents to this question indicated that English was not their first language and consequently they could not understand the verbose wording of the question. From the participants who did respond, six indicated that cracking software is justified if the software product is too expensive. Three believed that cracking software from a smaller company is not justifiable and, surprisingly, three believed that the benefits to end-users are not justified in any way.

With respect to the morality of software piracy, the responses suggest that most crackers have complex or confused attitudes regarding the morality of software piracy. Eight respondents challenged the morality of software companies in terms of their pricing and business strategies.

Phase 2: Cognitive interviews

In the interests of confirming the findings from the first phase of the study, the researchers conducted additional cognitive interviews. Gathering participants for these cognitive interviews was not easy. Just as the original participants were wary of participating in the survey, so too were these participants even more wary of a longer real-time interview exercise. In some cases it took weeks of careful trust-building and assurance using private messaging in order for the participant to agree to even a brief interview. As one participant reasoned, "if I was you and I wanted me to be comfortable enough to admit to something and then stay put while I did it, I'd use IRC". However, interview

TABLE VII

Desire for personal challenge

Code	Freq	Example
Stimulus: *Do you find the difficulty of cracking software a compelling reason to continue the activity due to the challenge involved?*		
Challenge is critical	19	"I know of no cracker who does not enjoy the challenge" "If there was no challenge then it would become just as boring as playing tic-tac-toe"
Experience Leads to desiring less challenge	6	"In the early days I could spend several weeks on a super hard crack. Now I try to avoid those" "However, I began to get the 'rush' [from cracking] less and less as I became a more experienced programmer" "I don't like to struggle too much...I'm not that patient anymore"
The harder the challenge the better	6	"When you crack really hard software you feel like you are in heaven" "The harder the challenge the more gratification one gets when finished and the more addictive it becomes" "Cracking simple software is no fun"
New protections are the most fun	5	"Cracking difficult software is the ultimate fun - especially when the protection is something new and elegant" "If there were no new protections it would get rather boring"
Copy protections are futile	1	"It's not the difficulty that keeps us going, it's the fact that we can say, 'look, it's pointless trying to protect [your software]'"

TABLE VIII

Personal need for free software

Code	Freq	Example
Stimulus: *How often do you pay for your own software?*		
Buy if software is worthy	9	"If there's something I truly think is great then I buy it"
		"I pay only for software I find worthy"
		"There isn't much software I use frequently that is worth paying for"
Rarely pay for software	8	"Hardly ever. And why should I. If I need it and can crack it then good for me"
		"I've never paid for it"
		"Never, I have no professional reason to do so, and as I am a student, very little money to ease my conscience"
		"Not often. I'm from a poor software"
Buy software when financially viable	4	"[I pay for software] whenever I have the money to do so"
		"If I could afford it, I would pay for Windows and Visual Studio"
Buy all software	3	"I buy all software"
		"If I use something I buy it"
Use free software when possible	3	"I do tend to look for free software a lot"

participants appeared to be interested in the research: "This is by far one of the most exciting emails I've got as a cracker, that someone really bothers to care what I think and mean".

Interview participants were asked for the same demographic information as the original survey participants. Table XV shows this demographics information, where they were provided.

Each interview involved discussion of each aspect of motivation and justification, and these are presented below.

Desire for social participation
While there was moderate support for the proposition that the social aspects of the cracking scene are highly rewarding, there was very strong support for

TABLE IX

Tangible benefit

Code	Freq	Example
Stimulus: *Have you ever received any kind of tangible benefit (money, free internet access etc) as a result of removing copy protection from software? If so, what?*		
No tangible benefits	19	"No, and if offered, I wouldn't accept it"
		"No. I've never received one. And I don't think a real cracker would do so"
Hostile to those who receive tangible rewards	7	"Such people are lamers and parasites. Furthermore they should be jailed"
		"Everyone in my circle of friends absolutely rejects the idea of people making money off warez – this is an evil thing in our view, and is not permitted"
Offered tangible rewards	5	"I have been offered gifts such as money and free equipment"
		"[I have been offered] money, shell accounts, free mail and free webspace for example"
		"One [person] even offered me $1500 for a patch"
Received tangible rewards to crack	3	"Yes, I have had someone pay me for my services"
Access to other pirated material	1	"Warez access"

the proposition that social participation is not a defining motivation factor for individuals to participate in software cracking. The responses suggest that, in the absence of a group environment, almost all (Mean = 6.33, Sig. = .000) respondents would continue cracking. Supporting this survey finding, Interviewee 3 noted, "We don't brag or make ourselves known as crackers to people outside of the groups." Interviewee 2 added confirmation to this,

arguing, "I don't tell others in real life, and I don't generally tell people outside my group. In fact, less than 10 people probably know what I do for the group". However, the effect of the cracking group appeared to be quite significant: one interviewee noted, "my wife just wouldn't understand".

Clearly there are other, more powerful, motivational factors if the respondents are so willing to continue cracking without the rewards offered by a

TABLE X

Denial of responsibility

Code	Freq	Example
Stimulus: *Does the disapproval of others influence the degree to which you participate in software cracking? If so, whose disapproval and in what capacity?*		
Not at all	18	"No. I participate in cracking for myself...No disapproval will change that. Some things should be done for yourself" "None, Whatsoever"
Do not care what others think	6	"I don't care one way or the other"
Never received disapproval	2	"I've never received any disapproval from anyone" "No one disapproves of it"
Opinions of software authors matter	1	"Software developers should be supported with cash" "I care about what they think – it's their effort."
Opinions of other group members matter	1	"[A crack] may not get released if the leader in the group I'm in doesn't want it to be"
Stimulus: *Does the threat of punishment affect your decision to continue cracking software? If so, how?*		
Punishment has no effect	11	"No, some get caught and made an example of, but it's not often and everybody involved is careful." "No the threat doesn't affect me at all. And why should it?"
Threat of punishment significantly influences cracking	10	"I'm getting older with more responsibilities. While I could have afforded to have been busted a few years ago wen I was in college, I really cannot anymore" "Yes, been thinking a lot of retirement. I guess it's not worth it, to be busted and lose everything" "Yes when DoD got busted we all got scared and some people quit"
Punishment threat concerns but does not influence	6	"Maybe for 5 minutes sometimes, but it's a true hobby of mine, it's my life, I do it in ANY free time I have" "Old habits are hard to break" "I tried to quit numerous times but it's just not possible. You will lose many friends, the feeling when you break a new protection and all other benefits the scene has to offer"
Punishment threat has reverse effect	2	"If there was no threat of being caught, not many would bother cracking. It's the little kid syndrome, the more you tell him not to, the more he does it." "It stimulates me very much...I love doing things considered dangerous or forbidden." "Forbidden apple is the sweetest."

TABLE XI

The denial of injury

Code	Freq	Example
Stimulus: *Do you think that software companies suffer as a result of your actions? If so, in what capacity?*		
Piracy hurts companies	11	"They only suffer if their product is good and worthy of payment"
		"Of course they do. They lose millions because of [software piracy]"
Piracy does not harm software companies	6	"Companies are so rich that the piracy problem does not exist in their case."
		"No. People who cannot afford their software will not buy it at all"
		"No. Those who crack wouldn't have paid for the software anyway"
Conflicted about effect	5	"Software companies never, but maybe single authors who release their software independently..."
Piracy benefits companies	3	"Some medium-sized firms say their sales went up after their software got cracked"
		"Some surely benefit from the huge increase in customer base that can occur when a piece of software is widely pirated"

social environment. One interviewee reflected on his own experience to support this, arguing, "I could meet up with the ones that live near me, but I choose not to meet them as I have no real interest to". The role that inter-group competition plays in the motivation to crack software may also be limited to those who value being the first to release a piece of pirated software. One interviewee gave context to this, arguing that, "there is somebody who is one step behind you and if you stop, your whole night's work is pointless because second place doesn't exist in the scene".

Desire for social status
The willingness of crackers to perform their actions anonymously suggests that recognition plays only a minor role in the motivation to crack software. The issue of receiving recognition for cracking software appeared to polarise the respondents (Standard Deviation=2.239, Mean=3.17). While the majority considered recognition unnecessary, there was a cluster of respondents who believed that receiving recognition was extremely important. On reviewing the results, one interviewee candidly wrote, "I can see why you found this. Very few want to be known personally, but they don't mind being known by a [nickname]. Nicks are also useful [because] you can walk away from them, and set up alibis if the heat is on".

The importance of pseudonymous prestige was apparent in Interviewee 2's comment, "The better/

faster you are at cracking, the better groups you can join. The very best groups get access to sites on [gigabit] links with tens of terabytes of information dating back years. Being in a respected group instantly gets you a lot of respect amongst others involved in the scene". Discussing the importance of this group hierarchy, one interviewee noted, "it's a training ground for the next generation".

Desire for personal challenge
Almost all survey respondents signalled that the harder a piece of software is to crack, the more enjoyable the experience. Almost all respondents (Mean 6.17, Sig. = .000) stated that releasing the software was secondary to the challenge of cracking itself. This finding was supported in the cognitive interviews. For instance, Interviewee 1 noted, "being one step ahead of the [software] developers is good for my ego. Basically, I'm better than them!". Interviewee 6 argued that, "We are just like you. You say you're doing this research just to find things out about the world. If you want to know what motivates us, look in the mirror". On reviewing the results, an interviewee wrote, "there is never a shortage of people willing to spend early in the morning hours of their time proving a point".

For some interviewees, this desire had persisted for some time. For instance, one respondent noted that "I still remember the huge mental rush I got from cracking my first program" and that "my parents actually supported me from the beginning

TABLE XII

The denial of the victim

Code	Freq	Example
Stimulus: *Does the size of a software company affect your decision to crack their software? Please explain your answer.*		
Size of a company affects decision to pirate software	12	"Yes. We all like to release well known titles. When you release good well known software you get more status!"
Size of a company does not affect decision to pirate software	12	"No, not at all, I crack whatever I can get my hands on" "Never, the software company has absolutely nothing to do with whatever I crack" "The size of the company is not a factor, solely their product or business morals"
Will not crack software from a 'small' company	8	"It does not trouble me when cracking very expensive apps from big companies, as I don't think I am costing them any money" "I try not to crack software made by poor students etc" "Yes. The small companies are usually working on a shoestring budget. The multinationals, well, they're a different kettle of fish..."
Will not crack software from a 'big' company	4	"Yes, we don't touch Microsoft, Adobe, MYOB...We leave the big fish to the big fish" "I would not go crack something from Adobe, they got money and power, and god knows what they would do"
Stimulus: *What role do the actions of the software industry play in the popularity of pirated software nowadays?*		
No role	6	"I don't think the actions of the software industry play any role in the popularity of pirated software. People like free stuff, and if their morals are at a certain level, they will use pirated software" "I don't see anything they do [in the Internet piracy environment] except of course developing the software" "They haven't got a role. If someone gets their hands on something unreleased it will get released. It's just a matter of time and motivation"
Remedy bad company practices	5	"If a company decides not to offer free updates that provides a strong incentive to crack their application" "Maybe if they protected their software a bit more then they wouldn't have a problem"
Over-pricing effects	5	"I doubt Windows would have been pirated in this large scale if it was cheaper" "How they can justify someone paying $1500 for a CD is ridiculous" "Companies demand too much for their products, that's why people use cracked stuff" "High prices of software is the main reason why so many people use pirated software"
Morally corrupt industry	2	"Should morally corrupt industry players attempt to crush the scene, it then becomes a game and they should expect a fight. The more they fight the more I will crack those players' software"
Self-destructed by advertising piracy	1	"The software and music industry have hurt themselves by making such a public issue out of file sharing clients like the former Napster and Kazza. Prior to the Napster controversy, few people realized that you could obtain music and software for free using these programs"

and I would like to consider myself to have developed into an ethical cracker''.

Personal need for free software
There was strong support in the survey (Mean = 2.21, Sig. = .001) for the proposition that crackers do not limit themselves to software that they personally need. An interviewee wrote, ''Most of the targets I examine aren't pieces of software that I even have any practical use for''. Echoing comments from other participants, another interviewee wrote, ''Nope, I release anything I can get''. The same interviewee also noted that he paid for software frequently: ''Every single

week. Last week I bought three programs costing $40–80 each''.

It is possible that some crackers apply a different set of reasoning to choosing software to crack and to personally using cracked software. Respondents may be reluctant to use cracked software if they see merit in its purchase, if they have the money to purchase the software, or if they are one of the three who purchase all their software. Supporting this contention, one interviewee noted, ''I actually buy games just to study their protections to an almost obsessive point. [I have] stacks of games on my shelf never played before but all with a different protection version''.

TABLE XIII

The condemnation of the condemners

Code	Freq[†]	Example
Stimulus: *What is your opinion of the reaction and response of the commercial software industry towards software piracy?*		
CSI have the wrong priorities	7	''Their reaction is wrong. They should make prices lower so that more people want to by a legal copy''
		''Developers should learn how to protect their software better''
		''They have made a mistake by making a public issue of the file-sharing clients
The CSI reaction is pointless	6	''They don't get it. The more you fight it, the more people will get into it, there is never a shortage of people willing to spend early in the morning hours of their time proving a point''
		''They are plain stupid. Targetting P2P-users won't lead anywhere''
Commercial software industry (CSI) ignore the issue	5	''Big companies seem to completely ignore the issue of cracking, almost as if they do not believe it hurts profits''
		''Do they react? I've rarely seen anything.''
CSI reaction is appropriate	2	''I support the BSA [Business Software Alliance] as they mainly crack down on companies that use pirated software''
Stimulus: *What is your opinion of the reaction and response of the law enforcement agencies towards software piracy?*		
Actions of law enforcement agencies (LEA) are justified	6	''They do their job, crackers are doing illegal actions''
		''They have a job to do''
		''Don't think they do anything wrong, they got the law on their side''
LEA have overreacted	5	''Their penalties are completely disproportionate to the crimes''
		''I think it's overkill''
Actions of the LEA are misguided	4	''Banning reverse-engineering will only cause a decline in computer security''
		''I would like to see law enforcement going into other areas, but I guess I would say that.''
		''Ridiculous. They should spend there [sic] resources on serious crimes like rape, murder and child abuse.''
		''If they actually understood why we crack then perhaps they'd employ us instead of putting us in jail''
LEA response is insignificant	4	''I'm always surprised there isn't more of a response''

[†] Two people signalled that they did not understand this question.

Public demand for free software

There was little evidence in the survey of altruistic concerns in the motivation of crackers. Further, there is evidence of a belief among crackers that individuals should pay for software that they use, (Mean=5.67, Sig.=.000). Interviewee 3 also commented on the curious relationship between crackers and the software-consuming public: "I don't care whether an end user is grateful to me, because I don't mean for them to be using the software in 99% of cases. They should be more grateful to the person that puts the release into the public domain (newsgroups, p2p)". Interviewee 2 noted, "I don't particularly care about what end users want, I'm more concerned with the competition side".

That crackers believe that others should pay for software they use, while the crackers themselves facilitate the use of pirated software by others, is something of a paradox. The attitude of crackers towards paying for software is clearly more complex

TABLE XIV

The appeal to higher loyalties

Code	Freq	Example
Stimulus: *Do the benefits to end-users justify the costs to software developers? If so, in what way?*		
Justified if software is too expensive	6	"Some software deserves the amount it costs, some software is just plain over priced"
		"Software developers should be reasonable in their prices, so that we leave their software un-cracked"
		"Some people from third world countries have the cracked software to train themselves with, giving them at east a chance to get employment"
Not justified with small companies	3	"The smaller the company, the less justifiable it becomes"
Benefits are not justified	3	"Software such as Adobe Photoshop has a reason for costing the price it does, because of all the features it has"
Stimulus: *Is software piracy morally wrong? Please explain your answer.*		
Ambivalent attitude	13	"I struggle with the moral issues of piracy – I have tried, not entirely successfully, to find a morally justifiable set of rules to follow"
		"I think it's a two sided story"
		"Well not really, it depends on how you think about it"
		"It depends on how you define software piracy"
Software companies are morally wrong	8	"The big companies and the existing laws against [piracy] are morally wrong, and piracy only flourishes because of the unnecessary high prices for software"
		"To keep a product for which you continually use is morally wrong, however, so is providing a product which is full of bugs and poor programming yet provided to the public without a money back guarantee"
Piracy is morally wrong	6	"Well, I think yes, ppl make a lot of afford to create software, and then smart arses like us crack it ;D"
		"Its basically stealing from people who work hard"
Piracy is not morally wrong	4	"I don't think it is seen as morally wrong, no more than breaching copyright when we copy a cassette tape or record a program off the TV"
		"No. What we do with the software should be up to us"
Only if it harms small firms	4	"I can understand a budding developer, working for a long time on a program and seeing his months of work given away on the net...in these circumstances I'd never release the program."
Only if for profit	3	"If you're making any kind of monetary or tangible profit off it, then yes"
		"If you are a company and use a software product to make money, then yes"

TABLE XV

Cognitive interview participant demographics

Interview Case	Gender	Age	Employment	Level of Education
1	M	31	Self-employed (no details)	B(Law), B(Comp. Sci.)
2	M	23	Medical Doctor	Graduate Bachelor of Medicine
3	M	18	Retail/Student	A-Levels
4	M	36	Software Architect	B(Comp. Sci.)
5	M	34	Not given	Not given
6	M	30	Financial Services	B(Commerce)
7	M	26	Not given	B(Arts)
8	M	44	Not given	PhD

than first thought. At the end of the interview, Interviewee 2 noted, "I would like to see 99% of end users without pirated software. If I had my way, scene releases would only be for those contributing to the scene".

Tangible reward

There was insignificant support (Mean=1.67, Sig.=.000) for tangible reward as a motivating factor to crack software. One interviewee made this comment regarding the tangible benefit finding: "cracking programs for fun and the challenge is morally right. Selling them in a organised group that passes pirate CDROMs is not only immoral but a criminal offence".

Interviewee 3 noted, "I've got a [power supply unit], cpu, 2 sticks of RAM and a hard drive. But that was a gift from the group, we don't get paid for cracking". Along similar lines, Interviewee 2 noted, "I had a friend in a group working in an ISP, he could get me free small Cisco routers, although I never took him up on the offer. Other than that, and the occasional bit of cash [via Paypal.com] for expensive software I couldn't afford, nothing other than site (FTP) access. That's all I ever wanted". Another argued, "I've only [received] the most important things: friendship and knowledge".

The interview stage proved valuable in that the researchers were able to probe the apparent duality between the insignificant effect of a tangible reward, and the significant dollar amounts attributed to software piracy globally. One interviewee explained, "walk through any street in Singapore or Hong Kong and you'll find stores full of CDs of Razor and Myth releases from the internet and newsgroups. We

all hate the idea of them making money in this way". Another explained, "Our group takes pride in perfect releases … this is a big thing in the scene … but by the time [the software] get to these pirate stores they are incomplete and full of trojans. Why would we want to be associated with that?". Another wrote, "it's just that it can be copied so easily … and they're just satisfying demand". Another interviewee noted, "selling cracked versions of software [is wrong] but I believe that … the software publishers are simply trying to charge as much as possible, without looking at what the software is actually worth to someone". This suggests that while crackers are integral to facilitating the spread of pirated software, through removing copy protection, the distribution of this software outside the group is conducted by other parties.

The denial of responsibility

The survey evidence demonstrated that the disapproval of the commercial software industry and law enforcement respectively had little influence on the decision to crack software. There was strong support for the argument that crackers accept full responsibility for their actions and the disapproval of others. In the case of crackers, the denial of responsibility is not used as a technique of neutralisation. One interviewee spoke of this with respect to their own cracking group's actions: "[Our group] has a note in the NFO that says something like, 'if you want us to stop cracking your software please contact us'. How many have contacted us in the last 2–3 years? 2–3 people? The authors don't know cracks exist or they just don't bother to look at them".

However, the interviews also showed that industry disapproval was not ignored altogether. On this issue, Interviewee 1 noted, "I personally have pretty high morals, but if you read the licence agreements in some software they state that you can't do this or you can't do that with the software. They are clearly trying to both have the cake and eat it. If I pay $1500 for software it should be mine to do what I want with. For example, a car manufacturer can't tell you not to repaint the expensive car you just bought". Other interviewees made similar comments. This suggests that crackers are aware that they are responsible for their actions (and hence do not deny responsibility), however, at the same time they feel as though there is a justifiable basis for this activity.

The denial of injury

While some respondents appeared to accept that their actions as a cracker cause harm to the software industry, some individuals believed their actions are harmless, or were, at least, conflicted about the existence of adverse effects. The interviews gave greater insight into this finding. One interviewee noted, "I have not harmed anybody and nobody has died from my actions, I believe piracy has never harmed real down to earth people, so what if some company earns 32 million rather than 54 million?".

However, some respondents did utilise the denial of injury to justify their actions. These respondents used the denial of injury to neutralise the fact that their actions run counter to law. For instance, on discussing the survey findings, one interviewee noted, "It also bothers me immensely that you could go to jail for cracking for longer than people go to jail for rape. To me that is a perversion of justice." Similarly, Interviewee 1 noted, "If I was to kill someone while DUI, I would probably get sent to prison for a year or so and get a $5,000 fine. If I copy/crack software I could go to jail for five years and get a fine of $10 million. Why is human life regarded as 'cheaper' than software? Mainly because the software industry lobby's [sic] our politicians and has a lot of money to do so". Another wrote that, "to bust them AND give them a fine comparable to manslaughter is just outrageous".

The denial of the victim

The survey results for the denial of the victim appeared to indicate that some thought the software industry did not deserve to have its products illegally copied. Interviews shed further light on this finding. One interviewee wrote that "the one comment ... that lingers with me and troubles me, is a comment about how pirated software might negatively impact the open source/free software community. The argument is that open source software would get more support and users if commercial software was not pirated, because it then becomes a more attractive alternative. I struggle with this issue".

However, some individuals believe that their actions as crackers are justified, regardless of any harm that their actions may cause. On whether software companies might suffer as a result of cracking activity, Interviewee 1 argued, "No, they don't. Bill Gates is still the richest man in the world". There is evidence of the denial of the victim as a neutralisation technique. This suggests that crackers may be capable of recognising targets they believe are inappropriate. Further research into the use of this technique is needed.

Condemnation of the condemners

The results of this factor suggest a divide in how crackers regard the software industry. While the majority of crackers do not wish any harm on the software industry as a result of their actions, there is a cluster of crackers who feel quite differently. Some respondents clearly felt that law enforcement agencies over-react in their interactions with crackers. For instance, on reviewing the survey results, one interviewee noted, "this will only challenge the cracker to release. They try to make stronger protections but forget to make their software near bug free, which is what the client wants. And that is what they will pay for. Not a very protected box of bugs".

Respondents were also critical of Microsoft's product and practice. For example, one respondent wrote, "All software I keep I pay for, except Microsoft. I feel their product to be highway robbery in respect of their continued sale of software that is buggy and a great security risk for the general public". Again, the size of the software publishing firm might play a role in this effect. One interviewee wrote that "the big boys like Microsoft and Adobe

will always be targets no matter what they do''. Another noted, ''Microsoft is a special case, well hated company that sells horrible software to millions of people''. Additionally, one respondent noted, ''I'm not touching any titles from Microsoft, they got the resources to put pressure on any agency to hunt me down''.

The appeal to higher loyalties
The survey finding for this factor was unclear. While some respondents believed that being unable to afford a piece of software should not be a barrier to using that software, others also felt that people should have to pay for software. Some crackers appeared to use the appeal to higher loyalties, in this case serving the community by supplying software, as a means of justifying their behaviour.

However, the conflicting results of this factor indicate that the majority of crackers might justify piracy depending on the situation and may have developed quite intricate methods for doing so. For example, consider this interviewee's comment, when asked whether all software should be free: ''No, but that doesn't mean I have to pay $2000 for Photoshop either. Not only could I not afford it, but even if I couldn't I would just use the [free, open source] Gimp instead, but since I have access to both for free, Photoshop is by far the better choice''.

The cognitive interviews provided useful additional insight into this neutralisation technique, with some interviewees arguing that crackers could be of use to the software industry because of their technical skills. One interviewee wrote, ''In the end we always win one way or another and if companies want to save some money and increase their profit, they should use our suggestions''.

Discussion and conclusions

The findings, with respect to the study's research questions, were as follows
1. What factors motivate software crackers to remove the copy protection from commercial software?
Findings from the survey stage suggest that the difficulty of removing copy protection is a significant motivating factor. Evidence from the cognitive interview stage further suggests that this is the

dominant motivating factor, overshadowing the need for social participation or desire for social status. One interviewee wrote, ''[the difficulty] is exactly my motivation. They're all little puzzles. Riddles I like to solve. I don't care about the program that's around it''. The analysis also showed that the presence or possibility of a tangible reward was not a motivating factor. Evidence from the interview stage suggested that not only is monetary compensation or payment not a motivating factor, but some respondents reviled the idea of receiving payment for cracking software.
2. What factors do software crackers use to justify removing the copy protection from commercial software?
Factors of justification were less clear. Most respondents denied some responsibility for their activity. There was some evidence of denying the victim and denial of injury as neutralization techniques: in particular, some crackers felt little sympathy for the vendors of more expensive software products. With regard to condemning the condemners, some crackers appeared to disapprove of law enforcement agency behaviour, while others found their behaviour acceptable and understandable. However, most of the respondents did not wish to cause harm to the original software authors themselves (particularly if the author was from a small firm). With regard to the appeal to higher loyalties, there was evidence that crackers might justify their activities depending on the circumstances.

Implications for research

This paper makes a number of contributions to research in the areas of ethics and information systems. First, this research compiles a number of factors of motivation and justification that are found to be important in the actions of those that remove copy protection from commercial software. Second, this study is among the first to explore the *originators* of pirated software rather than the users and distributors of pirated software.

Third, in terms of research method this study makes several contributions. The solicitation of participants from carefully chosen forums on the internet was generally successful and yielded respondents directly relevant to the research topic. The study's

method highlighted the effectiveness and reliability of administering a survey over the internet. The combination of open-ended questions and Likert-scale questions was highly successful and yielded a richness of information that would not have been possible using a single collection method. Subsequent confirmatory interviews using the cognitive interview method also proved invaluable in validating earlier findings and lending weight to the study. For exploratory research, the effectiveness of using multiple data collection methods was confirmed.

Implications for practitioners

There are a number of contributions for software and information systems practitioners. Software developers should understand that regardless of the complexity of a method of copy protection, there is evidence that crackers will still try and break the copy protection, simply for the challenge it involves. Interview discussion revealed that crackers are driven by the challenge of surmounting the copy protection. This suggests that increasingly difficult copy protection can act as a significant motivator to software crackers. Interviewee evidence supported this: "The harder they make it to crack, the harder we will work to crack it. Look at Microsoft's attempt to activate its new OS online – held us back a bit but we got there in the end". If the challenge is important to crackers, the finding may not apply to other members of the piracy process whose role is not as challenging, such as couriers and suppliers (consistent with Lee, 2002).

If the development of copy protection methods is a costly process, developers could reconsider the feasibility and viability of this activity. In this regard, it would be tempting to argue that software firms should make their software easier to copy and reduce the difficulty of the challenge. To this end, one interviewee wrote "the difficulty is what drives me, if all of it were easy, I don't think I would still be doing this stuff today". Similarly, one interviewee hinted, "I never try to crack a program simpler than the last one, this would be a loss of time". Another wrote, "if I see the protection is really, really easy, I don't publish the crack".

With regard to software authorship, managers should understand that many of these crackers are quite sympathetic to the plight of software developers, particularly those from small software companies. For instance, one interviewee wrote, "only the opinions of shareware authors against cracking influences me, and I try to read what I can about their views". Approaching a cracker or cracking group to request that they cease cracking their software may yield positive results. Further, some respondents felt that they were doing the software firms a positive service by assisting in bug removal, and increasing the user base. This is consistent with the arguments of Conner and Rumelt (1991), where software pirates enable the spread of software and thus increase its user base. Givon et al. (1995: 30) write, "pirates play an important role in converting potential users into users of the software, many of whom legally purchase the software".

Implications for policy makers

Finally, in terms of policy developers, if the goal of policy development is to curb software piracy then the following contributions should be considered. Crackers understand what they do is illegal yet that is not a restraining factor for their actions. One interviewee wrote, "I fear nothing of punishment. Like Galileo expanded his knowledge despite the church, I do the same. I live to know more. No one can force me out of it". The harshness of penalties is effective as a deterrent to some crackers. Recent arrests of people from the online piracy environment have considerably influenced how crackers perceive their actions although there is little evidence of it curbing their actions. Policy developers should understand that crackers may differentiate from others in the online piracy environment in that their actions are motivated mainly by the challenge of cracking. Providing an alternate outlet for this desire for personal challenge is an area that should be explored by policy developers.

Limitations

This study is subject to a number of important limitations. First, the small sample size limited the analysis that could be performed on the data. Factor

analysis would have been particularly useful in examining response differences between different respondent types. Without factor analysis it cannot be seen if respondents are using one technique or if a minority are using all techniques.

The sample may not be representative of the cracker population. The survey was self-selective, and responses may not be generalisable beyond the respondent group (Simsek and Veiga, 2001). Further, respondent desire for secrecy and non-repudiation, owing to the illicitness of software cracking, may have prompted them to omit significant information. Survey data are only provided for a single time period. Surveys conducted at later times may give different results, especially in as dynamic an environment as the software market. The findings may be biased due to differences in geographical regions, as respondents from non-English speaking backgrounds seemed to struggle with the phrasing of some questions. Further, only crackers who read the relevant forums were included in the sample.

In the absence of published studies on software cracking, the research factors were carefully chosen from the literature on motivation, justification, end-user software piracy, and computer crime. The measures used in the survey, while subject to pre-testing and based on past measures when possible, may not be effective factor proxies.

A number of avenues for future research exist based on this study. This research suffered from a small number of respondents. Repetition of the study with more respondents would make the data analysis more effective with more complex statistical analyses. Alternatively, a case-study approach could be employed using particular groups. This approach would yield information on all types of online piracy environment participants, not just crackers. This approach could focus on the large groups that law enforcement agencies believe are responsible for 90% of the pirated software available on the Internet (US Customs Service 2001). Crackers exhibit complex decision-making procedures with regards to the morality of software piracy, purchasing software, and attitudes towards software companies, which suggest the use of a personal code for decision making. Research into the existence of a personal code in crackers, is needed. Such research should also consider the degree to which this code can be influenced by extraneous factors, such as laws and software company disapproval.

References

Adams, G. R. and J. D. Schvaneveldt: 1991, Understanding Research Methods, 2nd Ed., Longman Publishers.

Alderfer, C. P.: 1969, 'An Empirical Test of a New Theory of Human Needs', *Organizational Behavior and Human Performance* **4**, 142–175.

Al-Jabri, I. and A. Abdul-Gader: 1997, 'Software Copyright Infringements: An Exploratory Study of the Effects of Individual and Peer Beliefs', *Omega, International Journal of Management Science* **25**(3), 335.

Anastasi, A.: 1982, *Psychological Testing* 5(Macmillan Publishers, New York).

Anderson, D. R., D. J. Sweeney and T. A. Williams: 1987, *Statistics for Business and Economics* 3(West Publishing Co., New York, USA).

Ashforth, B. E. and F. Mael: 1989, 'Social Identity Theory and the Organization', *The Academy of Management Review* **14**(1), 20–39.

Barber, R.: 2001, 'Hackers Profiled – Who Are They and What Are Their Motivations?', *Computer Fraud & Security* **2001**(2), 14–17.

Barbuto, J. E. and R. W. Scholl: 1998, 'Motivation Sources Inventory: Development and Validation of New Scales to Measure an Integrative Taxonomy of Motivation', *Psychological Reports* **82**, 1011–1022.

Barnard, C.: 1938, The Functions of the Executive, Englewood Cliffs.

Cambanis, T.: 2002, 'Leader of Software Theft Ring Sentenced' The Boston Globe. 17 August.

Cheyne, T. L. and F. E. Ritter: 2001, 'Targeting Audiences on the Internet', *Communications of the ACM* **44**(4), 94–98.

Conner, K. R. and R. P. Rumelt: 1991, 'Software Piracy: An Analysis of Protection Strategies', *Management Science* **37**(2), 125–39.

Constant, D., L. Sproull and S. Kiesler: 1996, 'The Kindness of Strangers: The Usefulness of Electronic Weak Ties for Technical Advice', *Organization Science* **7**(2), 119–135.

Creswell, J.: 1998, *Qualitative Inquiry and Research Design: Choosing Among the Five Traditions* (Sage Publications Inc, Thousand Oaks, California, USA).

Dabney, D.: 1995, 'Neutralization and Deviance in the Workplace: Theft of Supplies and Medicines by Hospital Nurses', *Deviant Behavior* **16**, 313–321.

Dalton, D. R., C. M. Daily and J. C. Wimbush: 1997, 'Collecting 'Sensitive' Data in Business Ethics Research: A Case for the Unmatched Count Technique (UCT)', *Journal of Business Ethics* **16**(10), 1049–1058.

Davis, F. D.: 1989, 'User Acceptance of Computer Technology: A Comparison of Two Theoretical Models', *Management Science* **35**(8), 982–1003.

De Young, M.: 1988, 'The Indignant Page: Techniques of Neutralization in the Publications of Paedophile Organizations', *Child Abuse & Neglect* **12**(4), 583–591.

Deacon, D., A. Bryman and N. Fenton: 1998, 'Collision or Collusion? A Discussion and Case Study of the Unplanned Triangulation of Quantitative and Qualitative Research Methods', *International Journal of Social Research Methodology* **1**(1), 47–63.

Deci, E. L.: 1975, *Intrinsic Motivation* (Plenum Press, New York).

Denzin, N.: 1970, 'Strategies of Multiple Triangulation', in N. Denzin (ed.), *The Research Act in Sociology: a Theoretical Introduction to Sociological Method* (McGraw-Hill, New York), pp. 297–313.

Dillman, D. A.: 1978, *Mail and Telephone Surveys: The Total Design Method* (John Wiley and Sons, New York).

Dubin, R.: 1978, *Theory Building* (Free Press, New York).

Eining, M. M. and A. L. Christensen: 1991, '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* (Boyd & Fraser, Boston), pp. 182–188.

Eliason, S. L. and R. A. Dodder: 2000, 'Neutralization Among Deer Poachers', *Journal of Social Psychology* **140**(4), 536–538.

Etzioni, A.: 1961, *A Comparative Analysis of Complex Organizations* (Free Press, Glencoe).

Ford, M. E.: 1992, *Motivating Humans* (Sage Publications, Newbury Park).

Friedman, B.: 1997, 'Social Judgments and Technological Innovation: Adolescents' Understanding of Property, Privacy, and Electronic Information', *Computers in Human Behavior* **13**(3), 327–351.

Galliers, D.: 1992, *Information Systems Research* (Blackwells, Oxford).

Gauthier, D. K.: 2001, 'Professional Lapses: Occupational Deviance and Neutralization Techniques in Veterinary Medical Practice', *Deviant Behavior* **22**(6), 467–490.

Gilbert, A.: 2003, 'Extradition Sought for DrinkorDie Chief', ZDNet.com.

Givon, M., V. Mahajan and E. Muller: 1995, 'Software Piracy: Estimation of Lost Sales and the Impact on Software Diffusion', *Journal of Marketing* **59**(1), 29–38.

Glass, R. S. and W. A. Wood: 1996, 'Situational Determinants of Software Piracy: An Equity Theory Perspective', *Journal of Business Ethics* **15**(11), 1189–1198.

Gopal, R. D. and G. L. Sanders: 1997, 'Preventive and Deterrent Controls For Software Piracy', *Journal of Management Information Systems* **13**(4), 29–48.

Gopal, R. D. and G. L. Sanders: 1998, 'International Software Piracy: Analysis of Key Issues and Impacts', *Information Systems Research* **9**(4), 380–397.

Gopal, R. D. and G. L. Sanders: 2000, 'Global Software Piracy: You Can't Get Blood From A Turnip', *Communications of the ACM* **43**(9), 82–89.

Grover, V., C. Lee and D. Durand: 1994, 'Analyzing Methodological Rigor of MIS Survey Research From 1980–1989', *Information & Management* **24**(6), 305–318.

Heltsley, M. and T. C. Calhoun: 2003, 'The Good Mother: Neutralization Techniques Used by Pageant Mothers', *Deviant Behavior* **24**(2), 81–100.

Highland, H. J.: 1984, *Protecting Your Microcomputer System* (Wiley, New York).

Hinduja, S.: 2003, 'Trends and Patterns Among Online Software Pirates', *Ethics and Information Technology* **5**(1), 49–61.

Hollinger, R. C.: 1991, 'Neutralizing in the Workplace: An Empirical Analysis of Property Theft and Production Deviance', *Deviant Behavior* **12**, 169–202.

Joinson, A.: 1999, 'Social Desirability, Anonymity and Internet-Based Questionnaires Behavior Research Methods', *Instruments and Computers* **31**, 433–438.

Katz, D. and R. L. Kahn: 1966, *The Social Psychology of Organizations* (John Wiley & Sons, New York).

Klein, H. K. and M. D. Myers: 1999, 'A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems', *MIS Quarterly* **23**(1), 67–93.

Kotulic, A. G. and J. G. Clark: 2004, 'Why There Aren't More Information Security Research Studies', *Information & Management* **41**(5), 597–607.

Kwong, K. K., O. H. M. Yau, J. S. Y. Lee, L. Y. M. Sin and A. C. B. Tse: 2003, 'The Effects of Attitudinal and Demographic Factors on Intention to Buy Pirated CDs: The Case of Chinese Consumers', *Journal of Business Ethics* **47**(3), 223–235.

Labovitz, S.: 1970, 'The Assignment of Numbers to Rank Order Categories', *American Sociological Review* **35**(3), 515–524.

Lau, F.: 1997, 'A Review on the Use of Action Research in Information Systems and Qualitative Research'. Information Systems and Qualitative Research. L. A. Liebenau and J. Degross. London. 31–68.

Lee D., Lee I., Ahn J., Kong Y.: 2002, 'The Illegal Copy Protection Using Hidden Agent'. Eurasia-ICT 2002:

Information and Communication Technology, Pro-
ceedings. 832–841.

Lee, J.: 2002, 'Pirates on the Web, Spoils on the Street'
The New York Times. 11 July 2002: 1.

Lee, R. M.: 1993, *Doing Research on Sensitive Topics* (Sage,
London).

Lee, W. B. and T. H. Chen: 2002, 'A Public Verifiable
Copy Protection Technique for Still Images', *Journal of
Systems and Software* **62**(3), 195–204.

Likert, R.: 1932, 'A Technique for the Measurement of
Attitudes', *Archives of Psychology* **140**(June), 5–53.

Lim, V. K. G.: 2002, 'The IT Way of Loafing on the Job:
Cyberloafing, Neutralizing and Organizational Justice',
Journal of Organizational Behavior **23**, 675–694.

Limayem, M., Khalifa, M., Chin, W.: 1999, 'Factors
Motivating Software Piracy: A Longitudinal Study'.
Proceedings of the 20th International Conference on
Information Systems.

Loch, K. D. and S. Conger: 1996, 'Evaluating Ethical
Decision Making and Computer Use', *Communications
of the ACM* **39**(7), 74–83.

Locke, E. A.: 1968, 'Toward a Theory of Task Motiva-
tion and Incentives', *Organizational Behavior and Human
Performance* **3**, 157–189.

Logsdon, J. M., J. K. Thompson and R. A. Reid: 1994,
'Software Piracy: Is It Related to Level of Moral
Judgement?', *Journal of Business Ethics* **13**, 849–857.

London, H. I.: 1975, *Social Science Theory Structure and
Application* (New York Press, New York)

Mackenzie, K.: 2002, 'Jail for US Pirate', *The Australian*
16(July), 26.

Malhotra, M. K. and V. Grover: 1998, 'An Assessment of
Survey Research in POM: From Constructs to The-
ory', *Journal of Operations Management* **16**(4), 407–425.

Maslow, A. H.: 1943, 'A Theory of Human Motivation',
Psychological Review **50**, 370–396.

Mason, R. L.: 1989, 'MIS Experiments: A Pragmatic
Perspective The Information Systems Research Chal-
lenge', in I. Benbasat (ed.), *Experimental Research
Methods* 2 (Harvard Business School Press, Boston), pp.
3–20.

Mathison, S.: 1988, 'Why Triangulate?', *Educational Re-
searcher* **17**(2), 13–17.

Maude, T. and D. Maude: 1984, 'Hardware Protection
Against Software Piracy', *Communications of the ACM*
27(9), 950–959.

McClelland, D. C.: 1961, *The Achieving Society* (Van
Nostrand, Princeton).

Minor, W. W.: 1981, 'Techniques of Neutralization: A
Reconceptualization and Empirical Examination', *Jour-
nal of Research in Crime and Delinquency* **18**(2), 295–318.

Moore, P.: 2003, 'Steal This Disk: Copy Protection,
Consumers' Rights, and the Digital Millennium

Copyright Act', *Northwestern University Law Review*
97(3), 1437–1470.

Moores, T. T. and J. Dhaliwal: 2004, 'A Reversed
Context Analysis of Software Piracy Issues in
Singapore', *Information & Management* **41**(8), 1037–
1042.

Moores, T. and G. Dhillon: 2000, 'Software Piracy: A
View From Hong Kong', *Communications of the ACM*
3(12), 88–92.

Nosek, B. A., M.R. Banaji and A. G. Greenwald: 2002,
'E-research: Ethics, Security, Design, and Control in
Psychological Research on the Internet', *Journal of
Social Issues* **58**(1), 161–176.

Peretti-Watel, P.: 2003, 'Neutralization Theory and the
Denial of Risk: Some Evidence From Cannabis Use
Among French Adolescents', *British Journal of Sociology*
54(1), 21–42.

Piazza, P.: 2002, 'Law Enforcement Targets Warez Sites',
Security Management **46**(3), 34.

Pierce, M. A. and J. W. Henry: 1996, 'Computer Ethics:
The Role of Personal, Informal, and Formal Codes',
Journal of Business Ethics **15**, 425–437.

Rahim, M. M., A. H. Seyal and M. N. A. Rahman: 1999,
*'Software Piracy Among Tertiary Students In Brunei Dar-
ussalam: An Empirical Study'* (Australian Institute of
Computer Ethics Conference, Swinburne University
of Technology, Melbourne, Australia).

Rosenberg, V.: 1989, 'Software Theft and Copy Pro-
tection', *Library Journal* **114**(2), 46–47.

Schildkraut, J. S. and J. Gasper: 2000, 'Copy-Protection
System for Photographic Paper', *Journal of Electronic
Imaging* **9**(4), 556–563.

Scott, A. C., J. E. Clayton and E. Gibson: 1991, *A
Practical Guide to Knowledge Acquisition* 1(Addison-
Wesley Publishers, New York).

Shim, J. P. and G. S. Taylor: 1991, 'A Comparative
Study of Unauthorized Software Copying: Informa-
tion Systems Faculty Members' vs Practicing Manag-
ers' Perceptions', in R. Dejoie, G. Fowler and D.
Paradice (eds.), *Ethical Issues in Information Systems*
(Boyd & Fraser, Boston), pp. 189–199.

Sieber, J. E. and B. Stanley: 1988, 'Ethical and Profes-
sional Dimensions of Socially Sensitive Research',
American Psychologist **43**, 49–55.

Simpson, P. M., D. Banerjee and C. L. Simpson: 1994,
'Softlifting: A Model of Motivating Factors', *Journal of
Business Ethics* **13**, 431–438.

Sims, R. R., H. K. Cheng and H. Teegen: 1996, 'To-
ward a Profile of Student Software Piraters', *Journal of
Business Ethics* **15**(8), 839–849.

Simsek, Z. and J. F. Veiga: 2000, 'The Electronic Survey
Technique: An Integration and Assessment', *Organi-
zational Research Methods* **3**(1), 93–115.

Simsek, Z. and J. F. Veiga: 2001, 'A Primer on Internet Organizational Surveys', *Organizational Research Methods* **4**(3), 218–235.

Smith, M. A. and B. Leigh: 1997, 'Virtual Subjects: Using the Internet as an Alternative Source of Subjects and Research Environment', *Behavior Research Methods, Instruments and Computers* **29**, 496–505.

Software & Information Industry Association, 2000, SIIA's Report on Global Software Piracy 2000.

Solomon, S. L. and J. A. O'Brien: 1991, 'The Effect of Demographic Factors on Attitudes Toward Software Piracy', in R. Dejoie, G. Fowler and D. Paradice (eds.), *Ethical Issues in Information Systems* (Boyd & Fraser, Boston), pp. 168–181.

Sproull, L. and S. Kiesler: 1991, *Connections: New Ways of Working in the Networked Organization* (MIT Press, Cambridge).

Straub, D. W.: 1989, 'Validating Instruments in MIS Research', *MIS Quarterly* **13**(2), 147–169.

Strutton, D., S. J. Vitell and L. E. Pelton: 1994, 'How Consumers May Justify Inappropriate Behavior in Market Settings: An Application on the Techniques of Neutralization', *Journal of Business Research* **30**(3), 253–z260.

Sykes, G. M. and D. Matza: 1957, 'Techniques of Neutralization: A Theory of Delinquency', *American Sociological Review* **22**(6), 664–670.

Turner, J. C.: 1984, 'Social Identification and Psychological Group Formation', in H. Tajfel (ed.), *The Social Dimension: European Developments in Social Psychology* (Cambridge University Press, Cambridge).

Tyler, M.: 1984, 'Software Piracy – Only One Per Customer', *Datamation* **30**(5), 49.

US Customs Service, 2001, 'U.S. Customs Dismantles One of the World's Most Sophisticated Internet Piracy Networks', US Customs Press Release, Dec. 11, 2001.

Vernon, M. D.: 1969, *Human Motivation* (Cambridge-University Press, Cambridge).

Waldron, V. R.: 1986, 'Interviewing for Knowledge', *IEEE Transactions on Professional Communications* **29**(2), 31–34.

Wallach, D. S.: 2001, 'Copy Protection Technology is Doomed', *Computer* **34**(10), 48–49.

Winchester, H. P. M. and L. N. Costello: 1995, 'Living on the Street – Social-Organization and Gender Relations of Australian Street Kids', *Environment and Planning D-Society & Space* **13**(3), 329–348.

Winfree, L. T., G. L. Mays, J. E. Crowley and B. J. Peat: 1994, 'Drug History and Prisonization – Toward Understanding Variations in Inmate Institutional Adaptations', *International Journal of Offender Therapy and Comparative Criminology* **38**(4), 281–296.

Wold, G. H., and R. F. Shriver: 1989, Computer Crime, Rolling Meadows, Bankers Publishing Company.

Sigi Goode and Sam Cruise
School of Business and Information Management,
Faculty of Economics and Commerce,
Australian National University,
Canberra, ACT 0200,
Australia
E-mail: sigi.goode@anu.edu.au