

Research

Ethical Attitudes of Entry-Level MIS Personnel

David B. Paradise

Department of Business Analysis and Research, College of Business Administration, Texas A & M University, College Station, TX 77843-4217, USA

A survey examining the ethical attitudes of over 125 upper division undergraduate business students was administered. As this sample contains students from throughout the southwestern United States that will be accepting jobs in a matter of months this group is representative of entry-level employees in this United States area. Frequently, entry-level employees are naive regarding "accepted" corporate behavior. "Acceptable behavior" may be a particularly ambiguous concept in the information systems field, since the field is still relatively young and is evolving at a tremendously rapid pace. The survey focussed on situations containing computer-based systems and investigated motives of obligation, opportunity, and intent. Responses by MIS subjects are compared to non-MIS subjects. Some statistically significant differences between the groups appeared: non-MIS subjects felt programmers should be responsible for the inherent correctness of calculations embodied in programs, MIS subjects indicated stronger notions of professional responsibility, and MIS subjects were more tolerant on the issue of unauthorized software copying. These results indicate entry-level personnel should be given specific guidelines regarding acceptable corporate behavior.

Keywords: Ethics, MIS, Data Processing Personnel, Ethical Dilemma, Entry-Level Personnel.

Introduction

Although unethical behavior by corporate executives makes headlines, the misjudgments of lower-level staff may ultimately cost organizations more. Errors in judgment may not be spectacular, but they require managerial time and effort to correct. When an employee mishandles a client, uses bad judgment regarding confidential information, or acts in any other manner that reflects poorly on the organization, someone in a senior position must usually take corrective action. In some cases, the employee may not even realize that the actions are unacceptable. In cases where an employee must be dismissed, the organization loses its investment in training that employee.

An earlier study [20] determined that the existence of a computer-based system in an ethical "dilemma" influenced ethical decision-making processes. In this paper, the attitudes of approximately 125 undergraduate third and fourth year students concerning a series of ethical "situa-



David Paradise is Assistant Professor of MIS in the Department of Business Analysis and Research at Texas A & M University. He holds a B.S. in information and computer science and an M.S. in industrial management from Georgia Tech and a Ph. D. in business administration (MIS) from Texas Tech. Dr. Paradise's primary research interests are investigating means for applying artificial intelligence techniques in managerial domains and studying the impact of technology on society. His research includes investigating methods of dynamic model construction in managerial advisory systems and utilizing qualitative models of organizational systems, as well as investigating the influence of computer-based information systems on ethical decision-making processes. Aspects of his research have appeared in the *Journal of Management Information Systems*, *Annals of Operations Research*, *IEEE Transactions on Systems, Man, and Cybernetics*, *Decision Sciences*, *Information Resources Management Journal*, and *Journal of Education in Business*.

North-Holland
Information & Management 18 (1990) 143-151

tions" involving computer-based systems are evaluated. Thus, these subjects represent a subset of the next one-to-two year population of entry-level employees in the southwestern United States.

Ethics Research in MIS

Although pursued widely [1,2,8,9,10,12,13,23,26,27,28,30] in other fields, ethics research is virtually nonexistent within MIS. However, the need for MIS-oriented ethics research has not gone unnoticed. Sackman [24] observed that ethics and values could be treated as research hypotheses and therefore examined scientifically. Weinberg [29] noted that data processing managers must deal with moral dilemmas but did not examine how data processing (i.e., MIS) professionals differ from others.

The Fourth National Conference on Business Ethics focused on ethics and computer technology management [11]. Topics included the application of existing ethical behavior codes in computer-based environments, the categorization of the computer as an inherently amoral tool, and the potential domination of computer professionals over others. The results of Parker's study of professionals (technologist, manager, ethical philosopher, lawyer, etc.) judging ethical issues in hypothetical scenarios indicated that their perception of ethical behavior varies widely [21,22]. In most cases, professionals were divided when asked whether the "actor" had behaved ethically. In some cases, they indicated there was no ethical issue. Parker's results indicate that differences may exist in the way these professional groups "process" a moral dilemma.

Recently, monographs have appeared on ethics and computers. Johnson [17] addressed issues involving the proliferation of computer-based information. He focused primarily on the need for modification of existing rules of human behavior. His work outlined characteristics that an "ethic for a computer society" should exhibit. Johnson [15,16], a philosopher, identified ethical issues of computer use from a contemporary philosophical viewpoint. She briefly reviewed competing ethical theories and examined several professional computing industry codes of ethics. She considered liability aspects for malfunctioning computer programs, conflicting societal concerns (e.g., informa-

tion need versus privacy rights) and the potential power derived by controlling information and access to it. This work identified issues but did not investigate them empirically.

Mason [18] addressed ethical behavior in terms of privacy, accuracy, property, and accessibility. There are data items which individuals have a right (1) to keep private, (2) to ensure are accurate, (3) to own, and (4) to access. He noted that "information forms the intellectual capital from which human beings craft their lives and secure dignity" [18]. However, information technology may be misused in all areas, reducing an individual's intellectual capital.

Recently, papers addressing MIS ethical issues have begun to appear. For example, Sheridan [25] investigates computer crime phenomena and asks whether an information system's presence directly impacts criminal activity. Jastrow [14] addresses the growth of computing power and relates this growth to man's evolution. He suggests that the future may consist of a symbiotic relationship, where computers minister to man's social and economic needs. Neither discussion, however, tests these hypotheses.

A recently formed professional organization in the United States emphasizes the ethical responsibilities of computer industry professionals. Computer Professionals for Social Responsibility (CPSR) is "an alliance of computer professionals concerned about the impact of computer technology on society." It is "a public interest organization of people in the computer field who are concerned about some of the current and proposed uses of computer technology." This group sponsors an annual conference and it reflects a growing concern by computer industry professionals for their impact on society. An industry newsletter, *Conscience in Computing*, is devoted to providing a forum for the discussion of ethical issues in computer-based environments [3].

In summary, while there is considerable and growing interest in computer ethics, empirical investigation of computer industry professionals' ethical decision-making behavior is scarce. As noted by Trevino, this circumstance is not surprising. Few managers would be willing to allow their ethical behavior to be monitored. And, manipulating ethical decision-making behavior in actual field studies would be unacceptable [27]. De George [6] observed that frameworks and hypotheses need to

be tested, however, to move business ethics research beyond discussions of morality to a point where tangible results that can impact organizational behavior can be identified.

Experimental Design and Data

Twelve ethical situations were developed and presented to subjects [see 4, 22]. The situations focus on three general areas: obligation, opportunity, and intent. These areas were chosen primarily because they have been identified in prior discussions as significant variables [e.g., 16, 22]. *Obligations* are one's responsibilities to others. *Opportunity* results from a favorable set of conditions to limit barriers or provide rewards [8]. *Intent* is defined as an individual's subjective probability that a behavior will occur [10]. It is determined by the individual's attitude toward the behavior [9].

As computer-based systems become more widespread, MIS entry-level professionals' perceptions of obligation becomes an important social issue. Since MIS entry-level personnel have technical skills that provide significant and powerful advantages in manipulating computer-based systems, opportunities exist for behaviors to evolve that are generally unacceptable to the larger part of society that does not possess these skills. Further, MIS staff access to systems provides an opportunity for unethical behavior that is generally unavailable to others. Organizational conflict may occur if the intentions of MIS staff diverge from corporate policies.

Twelve situations were presented to over 125 upper division undergraduate students in order to determine the attitudes of entry-level personnel. The subjects received no prior training or instruction, nor were they involved in any "consciousness-raising" discussion regarding ethics or ethical decision making. One person administered the instrument to all subjects. All subjects were voluntary, anonymous participants. Demographic data collected on age, sex, and socio-economic status of childhood environment revealed no statistically significant differences in the two groups. A religious fundamentalism survey [19] was also administered, again indicating no statistically significant difference in the groups.

Each subject was asked to read a situation, then answer a question regarding an actor in the situa-

tion. (Names were given to the scenarios to facilitate this discussion, these names did not appear in the original survey.) The subject was asked to indicate whether the actor's action was "unacceptable," "questionable," or "acceptable."

The subjects' responses were separated into MIS and non-MIS groups. Inclusion in either group was dictated by the subject's major area of study. In cases where a subject is pursuing a dual major (e.g., MIS and Accounting), the subjects were instructed to indicate which major they preferred to be associated with. The distributions of these responses were then analyzed using a chi-square test for independence to determine if the distributions were significantly different.

Discussion and Implications for Management of MIS Personnel

Each category of situations are now presented. Responses are presented and discussed, followed by comments on implications. The first category, containing four situations, addresses obligation.

Obligation of Responsible Use. A student had access to the university computer system because a class she was taking required extensive computer usage. The student enjoyed playing games on the computer, and frequently had to request extra computer funds from her professor in order to complete her assignments.

The student's use of the computer to play games was

	Unacceptable	Questionable	Acceptable
NON	64%	29%	7%
MIS	66%	23%	11%

Both groups indicated that this behavior was unacceptable. However, game playing was not the problem perceived by some. One subject indicated that game playing is acceptable *after* work has been completed. This subject seems to be objecting to playing before completing the assignments. Another subject indicated that game playing was acceptable but exhausting the computer funds was not. Apparently, had the student managed the game playing activity more responsibly, the behavior would have been acceptable to this subject.

Obligation of Responsibility. An engineer needed a program to perform a series of complicated calculations. She found a computer programmer capable of writing the program, but would only hire the programmer if he agreed to share any liability that may result from an error in the engineer's calculations. The programmer said he would be willing to assume any liability due to a malfunction of the program, but was unwilling to share any liability due to an error in the engineer's calculations.

The programmer's position in this situation is

	Unacceptable	Questionable	Acceptable
NON	9%	19%	72%
MIS	2%	8%	90%

The difference in the distribution of these responses is statistically significant ($p = .03$).

The engineer's position in this situation is

	Unacceptable	Questionable	Acceptable
NON	36%	29%	35%
MIS	61%	28%	11%

The difference in the distribution of these responses is statistically significant ($p = .005$).

Although a very slight majority of the non-MIS subjects agreed with the programmer in this scenario, the MIS subjects were much more clearly supportive of the programmer. The differences in the distribution of responses are strongly statistically significant in both questions. The difference in the two groups is most notable in the second question.

Obligation of Acknowledgment. A scientist developed a theory that required construction of a computer model to prove. He hired a computer programmer to build the model, and the theory was shown to be correct. The scientist won several awards for the development of the theory, but he never acknowledged the contribution of the computer programmer.

The scientist's failure to acknowledge the computer programmer was

	Unacceptable	Questionable	Acceptable
NON	67%	28%	5%
MIS	51%	38%	11%

The majority of both groups felt that the programmer should be recognized for his contribution to the scientist's success. However, the MIS subjects' responses are not as emphatic. This result could indicate that the non-MIS subjects value the skills of the programmer more than the MIS subjects.

Obligation to Client. The owner of a small business needed a computer-based accounting system. One day, he identified the various inputs and outputs he felt were required to satisfy his needs. Then, he showed his design to a computer programmer and asked the programmer if she could implement such a system. The programmer knew she could implement the system because she had developed much more sophisticated accounting systems in the past. In fact, she felt this design was rather crude and would soon need several major revisions. But, she didn't say anything about her feelings because the business owner didn't ask her and she thought maybe she could be the one hired to implement the needed revisions later.

The programmer's decision not to point out the design flaws was

	Unacceptable	Questionable	Acceptable
NON	37%	56%	7%
MIS	64%	32%	4%

The difference in the distribution of these responses is statistically significant ($p = .01$).

Again, the groups differ in a statistically significant manner. The majority of the MIS subjects felt that the programmer's behavior was unacceptable. Apparently, they have a professional ethic that requires them to provide the best service possible to a client. The non-MIS subjects were not so clearly decided on this one. The majority found the programmer's action questionable. Corporate conflict could occur in this type of situation if, for example, an MIS staff person felt more work was required to adequately complete an assignment, but a manager in another functional area perceived the work as unnecessary. The MIS employee could experience job dissatisfaction in this situation.

Regarding obligations, the responses appear to indicate that there is a general belief that computer resources should be utilized responsibly, that

programming consultants should provide high quality service, and that programming professionals should take responsibility for their work but should not be expected to assume responsibility for actions beyond their control.

The results indicate that entry-level MIS personnel generally feel obligated to provide a high quality product. One would expect that little effort should be required to create a quality control environment in which entry-level MIS personnel participate actively. Generally speaking, however, MIS entry-level personnel see no harm in utilizing corporate resources for personal motives that are not income producing. MIS management should make clear the corporate policy regarding this type of activity.

Relative to others, MIS entry-level personnel may generally perceive less value in their product. This perception may lead to increased self-doubt about the employee's contribution to the organization, and consequently to decreased job satisfaction [7]. While all management should occasionally praise lower level employees' work, the results indicate that MIS management should be especially careful to do so. Also, in matrix organizations where project teams may be formed combining staff from many corporate functions, MIS management should be careful to control the demands placed on MIS staff by other managers.

The next four situations address issues of opportunity.

Opportunity for Unauthorized Access. A student suspected and found a loophole in the university computer's security system that allowed him to access other students' records. He told the system administrator about the loophole, but continued to access others' records until the problem was corrected two weeks later.

The student's action in searching for the loophole was

	Unacceptable	Questionable	Acceptable
NON	28%	41%	31%
MIS	19%	51%	30%

The student's action in continuing to access others' records for two weeks was

	Unacceptable	Questionable	Acceptable
NON	87%	12%	1%
MIS	89%	11%	0%

The system administrator's failure to correct the problem sooner was

	Unacceptable	Questionable	Acceptable
NON	34%	58%	8%
MIS	43%	51%	6%

The majority of MIS and non-MIS subjects questioned the acceptability of searching for a loophole in the computer's security system. However, thirty per cent of each group felt that this action was clearly acceptable. One subject commented that the question did not reflect his interpretation of the situation; he felt "searching" for a loophole stated the case too strongly. Regardless, continued exploitation of the security problem was overwhelmingly perceived as unacceptable behavior by both groups. Both groups indicated the system administrator should have responded more quickly to the situation. One subject explained his "acceptable" response, however, by noting that the administrator may have been too busy to get to the problem immediately.

Opportunity to Obtain Software. A computer user called a mail order computer program store to order a particular accounting system. When he received his order, he found out that the store had accidentally sent him a very expensive word processing program as well as the accounting package that he had ordered. He looked at the invoice, and it indicated only that the accounting package had been sent. The user decided to keep the word processing package.

The user's decision to keep the word processing package was

	Unacceptable	Questionable	Acceptable
NON	31%	48%	21%
MIS	47%	38%	15%

Although not statistically significant, there appears to be greater intolerance for this action by MIS subjects. Almost half of the MIS subjects indicated keeping the word processing software was clearly unacceptable. The non-MIS subjects appear unsure; almost half labeled the action questionable.

Opportunity for Disruptive Behavior. A manager of a company that sells computer processing services bought similar services

from a competitor. She used her access to the competitor's computer to try to break the security system, identify other customers, and cause the system to "crash" (cause loss of service to others). She used the service for over a year and always paid her bills promptly.

The manager's actions were

	Unacceptable	Questionable	Acceptable
NON	97%	1%	1%
MIS	98%	0%	2%

Both groups were quite clear in their stand on this issue. The manager's behavior is unacceptable. Regardless of the manager's contractual legitimacy to access the competitor's system, the intent is clearly malicious and as such is considered unacceptable.

Opportunity Due to Privileged Access. A programmer at a bank realized that he had accidentally overdrawn his checking account. He made a small adjustment in the bank's accounting system so that his account would not have an additional service charge assessed. As soon as he made a deposit that made his balance positive again, he corrected the bank's accounting system.

The programmer's modification of the accounting system was

	Unacceptable	Questionable	Acceptable
NON	86%	11%	3%
MIS	90%	8%	2%

Both groups gave a strong indication that the programmer's action was unacceptable. This result may not be expected, however, since often individuals are allowed some latitude in their actions against organizations. Apparently, the subjects felt that the programmer's access to the system negated any latitude they may have otherwise allowed.

Generally speaking, "opportunity" in these situations can be more explicitly described as "opportunity to behave in a manner which will be undetected, or which is immune to retribution." In three of the situations, the opportunity for undetected access occurs. The other situation reflects opportunity for disruptive behavior which is protected by contractual agreement. Regardless of the situation, however, opportunity is not an accepta-

ble excuse for unethical behavior. Across all of these situations, the MIS subjects generally rejected behaviors as unacceptable based on the behavior, not on the likelihood of the behavior being detected. Based on these results, entry-level MIS personnel would not be expected to behave in a questionable manner due solely to the fact that the opportunity for such action may present itself.

The last four situations focus on the intent variable.

Use of Corporate Resource - Non-profit. A computer programmer enjoyed building small computer systems to give his friends. He would frequently go to his office on Saturday when no one was working and use his employer's computer to develop systems. He did not hide the fact that he was going into the building; he had to sign a register at a security desk each time he entered.

The programmer's use of the company computer was

	Unacceptable	Questionable	Acceptable
NON	11%	55%	34%
MIS	10%	52%	38%

The next situation is similar.

Use of Corporate Resource - Profit. A computer programmer built small computer systems in order to sell them. This was not his main source of income, he worked for a moderately sized computer vendor. He would frequently go to his office on Saturday when no one was working and use his employer's computer to develop systems. He did not hide the fact that he was going into the building; he had to sign a register at a security desk each time he entered.

The programmer's use of the company computer was

	Unacceptable	Questionable	Acceptable
NON	32%	45%	23%
MIS	40%	51%	9%

Here, computing resource misuse *for profit* is generally considered unacceptable behavior. The MIS subjects are much stronger in their indications in this regard. Although the majority of both groups in both situations are undecided about the

acceptability of using corporate computing facilities for personal use, there is a clear shift toward unacceptability when personal gain is intended.

Intent to Keep Copied Software. A student at a university learned to use an expensive spreadsheet program in her accounting class. The student would go to the university microcomputer lab, check out the spreadsheet software, complete her assignment, and return the software. Signs were posted in the lab indicating that copying software was forbidden. One day, she decided to copy the software anyway so she could work her assignments at her apartment.

If the student destroyed her copy of the software at the end of the semester, her action in copying the software was

	Unacceptable	Questionable	Acceptable
NON	45%	35%	20%
MIS	23%	29%	48%

The difference in the distribution of these responses is statistically significant ($p = .002$).

If the student forgot to destroy her copy of the software at the end of the semester, her action in copying the software was

	Unacceptable	Questionable	Acceptable
NON	56%	39%	5%
MIS	31%	54%	15%

The difference in the distribution of these responses is statistically significant ($p = .01$).

If the student never intended to destroy the software at the end of the semester, her action in copying the software was

	Unacceptable	Questionable	Acceptable
NON	77%	20%	3%
MIS	69%	23%	8%

The first question's responses reflect a clear difference in the two groups. The MIS subjects are much more tolerant of copying the software for personal convenience. While the majority of MIS subjects consider this behavior acceptable, the majority of non-MIS subjects feel it is clearly unacceptable. There is a clear shift by the MIS subjects in the second question, however. Here, the MIS subjects are not as forgiving of the software "piracy." Still, the difference in the distribution of the two groups' responses are statistically

significant as in the first question. The third question indicates that the majority in both groups feel outright software copying is unacceptable. One subject apparently had a problem responding to this question. No response was given, only a comment written in the margin: "Ugh! I'm guilty."

Intent of Virus Program. A "virus" program is a microcomputer program (typically) that performs tasks that a user has not requested, or does not want to perform. Some virus programs erase all files on a disk, some just print silly messages. One day, a very good student programmer decided to write a virus program. Virus programs always make a copy of themselves on other disks automatically, so the virus will spread to unsuspecting users. The student wrote a program that caused the microcomputer to ignore every fifth command entered by a user. The student took his program to the university computing lab and installed it on one of the microcomputers. Before long, the virus had spread to hundreds of users.

The student's action infecting hundreds of users' disks was

	Unacceptable	Questionable	Acceptable
NON	96%	4%	0%
MIS	98%	2%	0%

If the virus program output the message "Have a nice day.", then the student's action infecting hundreds of users' disks would have been

	Unacceptable	Questionable	Acceptable
NON	55%	31%	14%
MIS	60%	36%	4%

If the virus erased files, then the student's action infecting hundreds of users' disks would have been

	Unacceptable	Questionable	Acceptable
NON	96%	4%	0%
MIS	96%	4%	0%

All subjects generally agreed that spreading the virus that affected command processing was unacceptable behavior. But, spreading a nondestructive virus caused a perceptible shift in many of the subjects' minds. A number of non-MIS subjects even rated this behavior acceptable. Although the

Table 1
Managerial implications of survey results

Situation	MIS Managerial Implication
Obligation of Responsible Use	MIS entry-level personnel generally responsible.
Obligation of Responsibility	Responsibilities of MIS staff may need to be clearly delineated to other functional areas.
Obligation of Acknowledgment	Contributions of MIS personnel should be explicitly recognized. MIS personnel may undervalue work.
Obligation to Client	MIS entry-level personnel may feel conflicts regarding amount of work that should be performed. Policies outlining acceptable levels of service should be provided.
Opportunity for Unauthorized Access	System loopholes may be sought but exploitation of them is unacceptable. Policies for reporting and fixing security problems should be clear.
Opportunity to Obtain Software	MIS management may need to emphasize to staff that keeping unauthorized software is a crime.
Opportunity for Disruptive Behavior	All entry-level staff overwhelmingly reject any behavior that is disruptive.
Opportunity Due to Privileged Access	Very few MIS entry-level staff would take advantage of their privileged access to systems.
Use of Corporate Resource, Non-profit	MIS management need to clearly state policies regarding personal use of corporate facilities.
Use of Corporate Resource, Profit	MIS entry-level personnel may use corporate resource for personal profit.
Intent to Keep Copied Software	MIS entry-level personnel may not realize implication of unauthorized software copying. Corporate position needs to be explicit.
Intent of Virus Program	Destructive behavior is unacceptable, nuisance behavior is questionable. Corporate policies need to be clear.

shifts occur in both groups, fewer MIS subjects found the behavior clearly acceptable.

Generally speaking, "innocent" acts are acceptable, while "malicious" acts are not. MIS management should clearly specify to MIS staff the boundaries of "acceptable" behavior to reduce the risk of innocent acts at the entry-level becoming major corporate problems at higher organizational levels. The MIS responses generally indicate that deceptive practices or actions clearly intended to result in personal gain are unacceptable.

Table 1 summarizes the survey results and implications.

Conclusions

This study supports prior findings that differences exist between MIS subjects and non-MIS subjects (e.g., [5]) in a sample representative of entry-level personnel in the southwestern United States. The survey responses indicate MIS and non-MIS groups perceive differences in the obligations of MIS staff, that opportunity is not a reasonable excuse for questionable behavior, and that some acts are acceptable or unacceptable based on

the actor's ultimate intent. Frequently, corporate policies, or contractual agreements, are not as ambiguous. For example, the responses indicate that many of our subjects consider copying software for convenience to be acceptable behavior, while most contractual agreements strictly forbid such action, regardless of motive. This type of misjudgment (i.e., believing an act to be acceptable when it is actually unacceptable) leads to embarrassing situations. Managers are required to explain their subordinates' actions. More importantly, these conflicts could lead to loss of goodwill by clients, ultimately leading to lost business opportunities for the organization.

MIS managers need to be particularly careful to make explicit corporate policies regarding ethical behavior. Because the information systems field is relatively young, expecting entry-level personnel to be inherently aware of ethical policies may be unreasonable. As technology expands into new areas, information systems managers must constantly re-evaluate how the technology use impacts others. While basic principles of "right and wrong" are generally stable, ethical policies that reflect technological impact may evolve with the technology.

References

- [1] Barnett, J.H. and M.J. Karson. Personal Values and Business Decisions: An Exploratory Investigation. *Journal of Business Ethics*, Vol. 6, No. 5, 1987, pp. 371-382.
- [2] Bommer, M., C. Gratto, J. Gravander, and M. Tuttle. A Behavioral Model of Ethical and Unethical Decision Making. *Journal of Business Ethics*, Vol. 6, No. 4, 1987, pp. 265-280.
- [3] *Computer Decisions*. Putting Conscience into Computing. Hasbrouck Heights, New Jersey, USA: Hayden Publishing, Vol. 17, No. 21, October 22, 1985, p. 26.
- [4] Couger, J.D. Providing Norms on Ethics to Entering Employees. *Journal of Systems Management*, Vol. 35, No. 2, 1984, pp. 40-41.
- [5] Couger, J.D., R.A. Zawacki, and E.B. Oppermann. Motivation Levels of MIS Managers and Their Employees. *MIS Quarterly*, Vol. 3, No. 3, September 1979, pp. 47-56.
- [6] DeGeorge, R.T. The Status of Business Ethics: Past and Future. *Journal of Business Ethics*, Vol. 6, No. 3, 1987, pp. 201-211.
- [7] Dittrich, J.E., J.D. Couger, and R.A. Zawacki. Perceptions of Equity, Job Satisfaction, and Intention to Quit Among Data Processing Personnel. *Information and Management*, Vol. 9, No. 2, 1985, pp. 67-75.
- [8] Ferrell, O.C. and L.G. Gresham. A Contingency Framework for Understanding Ethical Decision Making in Marketing. *Journal of Marketing*, Vol. 49, 1985, pp. 87-96.
- [9] Ferrell, O.C., L.G. Gresham, and J. Fraedrich. A Synthesis of Ethical Decision Models for Business. Working paper, 1988, Department of Marketing, Texas A & M University, College Station, Texas, 77843, USA.
- [10] Fishbein, M. and I. Ajzen. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Boston Massachusetts, USA: Addison-Wesley, 1975.
- [11] Hoffman, W.M. and J.M. Moore (editors). *Ethics and the Management of Computer Technology*. Proceedings of the Fourth National Conference on Business Ethics, Bentley College, Waltham, Massachusetts, 02254, USA, 1981.
- [12] Horrigan, J.O. The Ethics of the New Finance. *Journal of Business Ethics*, Vol. 6, No. 2, 1987, pp. 97-110.
- [13] Hunt, S.D. and S. Vitell. A General Theory of Marketing Ethics. *Journal of Macromarketing*, Spring, 1986, pp. 5-16.
- [14] Jastrow, R. Toward an Intelligence Beyond Man's. in *Information Systems for Management: A Book of Readings*. Watson, H.J., Carroll, A.B., and Mann, R.J., editors. Plano, Texas, USA: Business Publications, Inc. 1987, p. 512-514.
- [15] Johnson, D.G. *Computer Ethics*. Englewood Cliffs, New Jersey, USA: Prentice-Hall, 1984.
- [16] Johnson, D.G. Equal Access to Computing, Computer Expertise, and Decision Making About computers. *Business and Professional Ethics Journal*, Vol. 4, Nos. 3 & 4, 1985, pp. 95-103.
- [17] Johnson, D.W. *Computer Ethics: A Guide for the New Age*. Elgin, Illinois, USA: The Brethren Press, 1985.
- [18] Mason, R.O. Four Ethical Issues of the Information Age. *MIS Quarterly*, Vol. 10, No. 1, March 1986, pp. 4-12.
- [19] Martin, J. and F. Westie. The Tolerant Personality. *American Sociological Review*, Vol. 24, 1959, pp. 521-528.
- [20] Paradise, D.B. and R.M. Dejoie. An Investigation of the Influence of Information Systems on Ethical Decision-Making Behavior. Working paper, 1988, Department of Business Analysis and Research, Texas A & M University, College Station, Texas, 77843-4217, USA.
- [21] Parker, D.B. *Ethical Conflicts in Computer Science and Technology*. Menlo Park, California, USA: AFIPS Press, 1979.
- [22] Parker, D.B. Ethical Dilemmas in Computer Technology. *Ethics and the Management of Computer Technology*. Proceedings of the Fourth National Conference on Business Ethics, Bentley College, Waltham, Massachusetts, 02254, USA, 1981.
- [23] Robin, D.P. and R.E. Reidenbach. A Framework for Analyzing Ethical Issues in Marketing. *Business and Professional Ethics Journal*, Vol. 5, No. 2, 1988, pp. 3-22.
- [24] Sackman, H. *Computers, System Science, and Evolving Society*. New York, New York, USA: John Wiley and Sons, 1967.
- [25] Sheridan, J.H. Is There a Computer Criminal Working for You? in *Information Systems for Management: A Book of Readings*. Watson, H.J., A.B. Carroll, and R.J. Mann (eds). Plano: Business Publications, Inc. 1987, pp. 499-511.
- [26] The Business Roundtable. *Corporate Ethics: A Prime Business Asset*. New York, New York, USA: The Business Roundtable, February 1988.
- [27] Trevino, L.K. Ethical Decision Making in Organizations: A Person-Situation Interactionist Model. *Academy of Management Review*, Vol. 11, No. 3, 1986, pp. 601-617.
- [28] Vitell, S.J. and S.J. Grove. Marketing Ethics and the Techniques of Neutralization. *Journal of Business Ethics*, Vol. 6, No. 6, 1987, pp. 433-438.
- [29] Weinberg, G.M. *The Psychology of Computer Programming*. New York, New York, USA: Van Nostrand Reinhold Company, 1971.
- [30] Zey-Ferrell, M., M. Weaver, and O.C. Ferrell. Predicting Unethical Behavior Among Marketing Practitioners. *Human Relations*, Vol. 32, No. 7, 1979, pp. 557-569.