



The ethical attitudes of information systems professionals: outcomes of an initial survey

Mary Prior ^{a,*}, Simon Rogerson ^b, Ben Fairweather ^b

^a *Department of Information Systems, De Montfort University, The Gateway, Leicester LE1 9B, UK*

^b *Centre for Computing and Social Responsibility, De Montfort University, The Gateway, Leicester LE1 9B, UK*

Abstract

This paper presents the results of a survey of the ethical attitudes of information systems (IS) professionals conducted during 1998. Surveys of attitudes reported in the literature are outlined, then the research objective and methodology are described and the main findings are discussed. While the survey indicated a high level of ethical awareness among respondents, it also highlighted a number of problematical areas, tending to confirm the findings of previous surveys. Finally, suggestions for further research in this area are made. © 2001 Elsevier Science Ltd. All rights reserved.

Keywords: Computer ethics; Ethical attitudes; IS practice

1. Background

Interest in the question of ethical behaviour in the context of information technology (IT) has been growing over the past two decades, as evidenced by the burgeoning literature in this area. Pearson et al. (1996) suggest that it is appropriate to study the ethical behaviour of information systems (IS) professionals for three reasons. Firstly, as organisations become more strategically reliant upon IT systems, IS professionals' behaviour may have a significant impact on the future of their company. Secondly, decision-making is based upon available information, and IS professionals have direct responsibility for the quality of the information available to

* Corresponding author. Tel.: +44-116-255-1551; fax: +44-116-254-1891.

E-mail address: mprior@dmu.ac.uk (M. Prior).

decision-makers. Thirdly, in contrast to more established professional groups, IS professionals nationally have no single code of ethics to help guide their behaviour.

An early study was conducted by Parker (1979) who held a workshop during which he presented scenarios involving issues of computing ethics to a group of professionals, including computer scientists, with the goal of enhancing discussion about ethics. Participants in the workshop, who all had a strong interest in computer ethics, voted whether characters in the scenarios acted ethically, unethically, or whether no ethical question was involved. Paradice (1990) similarly used a series of 'ethical situations' to survey attitudes of two groups of students approaching graduation, one group being MIS and the other non-MIS students. He found some differences between the groups in terms of what they considered to be 'unacceptable', 'questionable' and 'acceptable' behaviour although this depended upon the issue, neither group being consistently 'more' nor 'less' ethical than the other. Vitell and Davis (1990a) examined the ethical behaviour of MIS professionals and the link between ethics and job satisfaction for this professional group (Vitell and Davis, 1990b). They mailed a questionnaire to practitioners requiring them to indicate whether they agreed or disagreed with a series of statements. They found a strong sense of social responsibility among the respondents and a positive correlation between job satisfaction and ethical behaviour.

The attitudes of computer science practitioners and one group of computing, and one of non-computing students were surveyed by Leventhal et al. (1992) using scenarios that were mailed to practitioners and distributed to students in class. These authors found that ethical attitudes developed as people gained experience and skill. They also found some gender differences in responses. Athey (1993) compared the attitudes of computing students to scenarios developed by Parker et al. (1990) with those of the 'experts' (i.e., computing professionals with some experience) who had first examined them. She found that students had significantly different ethical opinions from the older, more experienced experts. Conger et al. (1995) examined the attitudes of computer *users*, who were not necessarily IS personnel. Scenarios were presented to graduate students who rated actions as highly unethical, grey area or highly ethical. The findings indicated that respondents were consistently egocentric, lacking an awareness of other stakeholders. The researchers suggested that the use of technology forces a psychological separation of the user from other stakeholders and leads to unethical behaviour. At the same time, some consensus regarding what are 'correct' ethical actions was found and a need to develop more consensus identified.

The effect of codes of ethics on computer abuse judgements and intentions of IS personnel was discussed by Harrington (1996). Scenarios were given to employees, who were encouraged by their MIS managers to participate in the survey. It was found that codes of ethics had a small effect on computer abuse judgements and intentions for some issues, but that their effect was weak in comparison to the strong psychological trait of denial of responsibility. The findings suggested that management cannot control employee behaviour solely through codes of ethics.

Attempts to determine whether men and women have different ethical attitudes were made by Kidwell et al. (1987) and Kreie and Cronan (1998), with contradictory results. The former study used a self-administered questionnaire comprising a set of ethical decision situations that was delivered personally to subjects holding a managerial post. It was found that men and women respondents did not differ in their perception of what is not ethical. However, women were more likely to consider concealing one's own errors to be unethical and both groups considered the other to be more unethical than themselves. Kreie and Cronan (1998) presented five scenarios to students and found that men and women were distinctly different in their assessment of what was ethical and unethical behaviour, with men less likely than women to find certain behaviours unethical.

All of these surveys were conducted in North America. While providing a valuable contribution to an understanding of ethical behaviour in the context of IT, this work necessarily provides a view grounded in one particular context.

Evidence of the ethical attitudes of IS professionals operating in other parts of the world and the extent to which they converge with or diverge from those of practitioners in North America is lacking.

1.1. Research objective

A survey was undertaken by the Centre for Computing and Social Responsibility (CCSR) at De Montfort University, UK, on behalf of the Institute for the Management of Information Systems (IMIS), for whom a report of findings was prepared (Prior et al., 1999). The aim of the survey was to determine the views of members of the IMIS concerning a variety of ethical issues. It is believed to be the first large-scale study of the attitudes of IS professionals to have been conducted in the United Kingdom. As noted above, previous surveys published in the literature have been conducted in North America; this survey aimed to provide some evidence of the ethical attitudes held by members of one European professional association.

2. Methodology

Surveying people's attitudes is a difficult task; there is no objective way of validating the answers subjects give although with care, the reliability of the questions posed can be increased (Fowler, 1993). Given the resources available, it was decided that a self-administered questionnaire would be published in an issue of the *IMIS Journal*. As respondents were therefore self-selecting, they are not necessarily representative of IMIS membership as a whole, nor is the IMIS membership itself necessarily representative of all IS professionals; this limitation needs to be borne in mind in any interpretation of the results. It may be noted that only half of the

surveys referred to above used populations drawn from practitioners (as opposed to students) and of those, the participants in Parker's workshops were also self-selecting.

The majority of previous surveys followed Parker (1979) in using a series of scenarios of ethical decision situations, requiring respondents to judge to what extent various characters had acted ethically. This format was considered, but rejected for the CCSR survey. As it was to be distributed via publication in a journal and the respondents would be a self-selecting group, it was important to encourage as high a response rate as possible. The survey needed to seem quick and easy to complete; a series of scenarios might have deterred potential respondents by appearing to be time-consuming to work through, particularly as a large number of scenarios would have been necessary to cover a wide range of issues. Hence, it was decided to use statements, with respondents asked to indicate the extent to which they agreed or disagreed with each one on a Lickert scale (Oppenheim, 1966) with possible responses of '*strongly disagree, disagree, indifferent, agree, strongly agree*'. In total 21 statements were formulated (see Appendix A). For the majority of ethical issues, more than one statement was provided, approaching the issue from different angles, and in some cases distributed randomly among the statements to test the respondents' consistency of response. The issues covered, with the number of statements devoted to the issue, are

The importance of ethical considerations to organisations	(3)
The importance of ethical considerations to self	(2)
Intellectual property	(4)
Use of employer's computing facilities	(2)
Privacy	(2)
Security	(2)
Electronic surveillance of employees	(1)
Involvement of users and clients	(2)
Affect of computer system on work environment	(1)
Honesty to the client	(1)
Amount of testing effort	(1)

In addition to the 21 statements, 18 questions were devoted to Codes of Conduct, to determine whether the respondents' employing organisations had a code, how familiar the respondents were with the codes both of their employing organisation and their professional society, how useful they found these codes in practice and how relevant they consider Codes of Conduct to be to IS professionals.

Finally, eight questions were used to gather demographic data such as the respondents' gender, age and employment profile.

The questionnaire was piloted with a small group of IS professionals at the end of 1997, after which the statements and questions were refined. The questionnaire was

Table 1

Gender	%	Age	%	Time with current employer (in years)	%	Total time as an IS professional (in years) ^a	%
Male	88.2	Under 25	11.8	< 1	16.1	<1	9.5
Female	11.8	35–40	33.5	1–2	16.1	1–2	5.1
		41–50	33.5	3–4	19.3	3–4	10.2
		Over 50	21.2	5–9	21.7	5–9	8.0
				>10	26.7	>10	67.2

^aNote that half of the students did not answer the question concerning total time as an IS professional; of those who did answer, all but two said <1, the other two said 1–2 years.

validated by a professional market researcher and published in its final form in the March 1998 issue of the *IMIS Journal*.

A total of 170 responses were received. As indicated in Table 1, the majority of respondents were male and were experienced IS professionals. Two-thirds were aged between 25 and 50 years. There is evidence of job mobility in the profession; over half of the respondents had worked for their current employer for less than 5 years. Experience is also reflected in Table 2, which shows that more than a quarter of respondents said that ‘Manager/Director of IS’ best described their job title. Table 3 shows that more than half of the respondents worked for private enterprise,

Table 2

Job title	%	Job title	%
Manager/Director of IS	26.6	Programming Manager	0
Project Leader	5.9	Applications Programmer	4.1
Business Analyst	4.7	Systems Programmer	1.2
Systems Analyst	4.7	Lecturer/Teacher	3.6
Database Manager	2.4	Student	9.5
Technical Services Manager	4.7	Other	30.2
Network Manager	2.4		

Table 3

Employer’s business	%	Total no. of employees	%
Private enterprise: Computer industry	24.7	<10	18.7
Private enterprise: Non-computer industry	30.1	11–100	20.7
Public service	19.3	101–500	18.7
Academic	11.4	501–1000	8.7
Self-employed	7.2	1001–5000	18.0
Other	7.2	>5000	15.3

although the public sector was also quite well represented. There was an even spread of responses from different sizes of organisation.

3. Findings

Responses to each statement were totaled and cross-tabulation performed on characteristics such as job title, type of business, size of employing organisation, length of time spent as an IS professional and age. Some chi-square tests were performed on the data; however, it was found that the sample size was too small to provide reliable results. Thus, while trends in the responses can be noted, a larger population would have been required in order to determine the level of significance of the findings.

A summary of the responses will be found in Appendix A. Overall, they indicate a high level of ethical awareness. Since such a large proportion of the respondents were experienced personnel and they were self-selecting, this might have been expected. However, a number of problematical areas were highlighted and it is these and the extent to which the findings of this survey concur with those of previous surveys that will now be discussed.

3.1. Relationship between age/experience and attitudes

For several of the statements, there appeared to be a relationship between the respondents' age and their response. For example, in response to the statement, '*I would refuse to work on a project that I considered to be unethical*', a higher proportion of the under 25-year-olds *strongly disagreed*, and a higher proportion of the 25–40 age group *disagreed*, than the older age groups. Younger respondents were more likely than other respondents to agree or strongly agree with the following statements:

Employers are entitled to use electronic surveillance to monitor employees' performance without their consent.

If a project is significantly behind schedule or over budget, it is acceptable to cut down on testing effort.

It is acceptable for a software contractor, provided with a brief specification, to go ahead and develop the system knowing that in future re-work under another contract will be essential.

These responses are consistent with those made to other surveys. The students surveyed by Athey (1993) held 'significantly different ethical opinions than older, more experienced experts'. She speculated that this may have been due to the

students having had little work experience and not having given the issues much consideration; or that perhaps they feared a negative impact on their career if they challenged ‘unethical’ behaviour. Like Susan Athey, Couger (1984) reported using the Parker scenarios with students, whose responses differed significantly from those of ‘expert practitioners’; generally, scenarios considered by the latter to be ‘unethical’ were rated ‘not unethical’ or ‘no ethics issue’ by students.

Pearson et al. (1996) found that older, more experienced, IS professionals had developed a more mature understanding of ethical issues and concluded that they typically should have better insights into what is considered acceptable ethical behaviour by the IS professional. Barnett and Karson (1989) discovered career stage to have an important effect on attitudes; subjects at a later career stage were generally ‘more ethical’ in all scenarios presented to them. Leventhal et al. (1992) found evidence that the ‘development of attitudes is dynamic and ongoing as people gain technical expertise’.

Cross-sectional studies such as these cannot determine the cause of the difference in attitudes between different age groups. It may be that experience is a factor. It could also be that differences between age cohorts may be indicative of a shift in what is considered ‘ethical’ behaviour by society as a whole. It is possible that a major concern for younger professionals is the building of a career, and they therefore tend to be more pragmatic about the kind of work they accept than more well-established older employees. We are conducting further studies that may help to shed light on this issue.

These findings raise important issues for organisations and for professional societies, in terms of the need to support younger professionals at the start of their career and in terms of raising the ethical awareness of employees at all levels in an organisation.

3.2. *Use of employer’s IT resources*

While an overwhelming majority of the respondents considered it *not* acceptable to use their employer’s computing facilities for their own *profit-making* activities, opinions differed as to the use of the same facilities for *non-profit-making* activities. Nearly half (48.8%) either strongly agreed or agreed that use of facilities for non-profit activities was acceptable; 15.5% were indifferent and 35.7% disagreed or strongly disagreed. The statement did specify, ‘if this has no adverse effect on my employer’, implying use outside working hours or when the equipment was not in use for business purposes.

In the study conducted by Conger et al. (1995), respondents considered the taking of paper-clips to be more unethical than the use of computer resources for playing games or producing a sports club newsletter. There appeared to be a perception of a difference in unacceptability between taking physical items such as paper clips as compared to the use of an apparently free resource such as computer time. Several of the respondents stated that if the company had no policy, managers did not care

whether employees used computers for personal work; however, they admitted that this view might be disputed by company executives. Kreie and Cronan (1998) found over 80% of respondents agreeing that it was acceptable to use computer resources for personal use, in the employee's own time. Some respondents did indicate that company policy forbidding such use would cause them to change their judgement. Paradice (1990) similarly found that entry-level MIS personnel saw no harm in using corporate resources for personal non-profit activities, while the majority regarded use for profit as unacceptable.

The consistency of the results of these various surveys is interesting and highlights the need for a clear policy on the use of corporate resources by employees. Some organisations may wish to ban any personal use of their resources. Respondents make a clear distinction between the use of corporate resources for *profit* and *non-profit* activities; the evidence suggests that a ban on the former would be accepted as reasonable and justified by the vast majority of employees. The evidence also suggests that in the absence of any policy to the contrary, many employees may well be using corporate IT resources for personal use. One possibility would be for organisations to permit personal use within well-defined limits as a legitimate 'perk' for employees; for example by allowing use outside of working hours for employees working for local charity or community groups. A transparent policy of this nature would allow the organisation to monitor the non-work use of its facilities and to enhance its standing within the local community.

3.3. Privacy and security

When asked whether they considered it acceptable to use other employees' access codes to access data normally hidden from them, respondents made a clear distinction between whether they used others' codes *without* their permission (94.1% thought this *unacceptable*) or *with* their permission. In the latter case, 33.3% of respondents agreed or strongly agreed that this was *acceptable* and a further 7.1% were indifferent. The intention of the question was that the other person *permitted* the use of their access code but that the respondent was still not entitled to view the data. The phrase 'with their permission' in the question may have been taken by some respondents to imply the granting of authority to view data normally hidden from the respondent. Nevertheless, the findings suggest that a third of respondents were more concerned about having permission to use someone else's access code, than with whether or not they should have access to data normally hidden from them.

With respect to security, more respondents considered data held on computer systems to be at risk from *internal* rather than from *external* sources. The most significant relationship was with the job title of the respondent. The groups most frequently reporting data to be at threat from internal sources were Database Managers, Technical Services Managers and Network Managers. The findings seem to suggest that those most closely involved with the storage, access and transmission

of data had less confidence in security measures than the IS managers who responded to the survey.

Conger et al. (1995) found a minority of respondents who considered browsing through company files to be acceptable. The percentages varied according to the data involved: 11% thought browsing through others' e-mail was acceptable; 13% employees' medical files and 19% employees' salary files.

It is clear when the responses with respect to privacy and security are taken together, that security is not only a technical issue, but one with important human resource management implications. A sizeable minority of the respondents in these surveys appeared to see nothing wrong with using their data access privileges to infringe the privacy of others. This suggests that organisations need to scrutinise carefully their policies and practice relating to data access to ensure that curiosity does not lead to abuse of privilege.

3.4. *Electronic surveillance*

Over 20% of respondents agreed or strongly agreed that employers are entitled to use electronic surveillance to monitor employees' performance without their *consent*. As noted above, the responses appear to be related to age; the younger the age group, the higher the proportion of respondents who agreed with this proposition. It is a matter of concern that so high a proportion of respondents should be seemingly unaware of the ethical issues raised by workplace surveillance, in particular because it is IS professionals who are the employees likely to be called upon to design, install and maintain electronic surveillance systems.

Conger et al. (1995) asked a slightly different question with respect to electronic surveillance. They found that company monitoring of, for example, phone and email use by employees was considered to be unethical by 83% of respondents if it was *unknown* to employees. However, if the practice was *known* to employees, 33% of respondents considered the practice to be unethical, 37% ethical and 24% thought it to be a grey area.

Clearly, there is a need to raise awareness among IS professionals in particular, and perhaps among both employers and employees in general, concerning the ethical issues raised by electronic surveillance in the workplace. There is a need to define the rights of all stakeholders and to identify appropriate guidelines and standards for ethical practice in this area.

3.5. *Gender*

A number of studies have examined the extent to which gender is an influencing factor in ethical attitudes. However, there is little consistency in their findings. Kreie and Cronan (1998) surveyed the responses of men and women IS students at a midwestern university in the United States to a variety of scenarios. They concluded that, 'Men and women were distinctly different in their assessment of what is ethical

and unethical behaviour. For all scenarios, men were less likely to consider a behaviour as unethical.'

Leventhal et al. (1992) also found some differences in responses from men and women. However, Kidwell et al. (1987) surveyed men and women in comparable managerial positions and concluded that they generally did not differ in what they considered ethical and what they considered unethical; the only difference being a greater propensity for the males to conceal their errors. Barnett and Karson (1989) surveyed executives in an insurance company and found that not only was gender *not* the most significant effect on ethical decision-making, but that there was no consistency of effect; females made 'more ethical' decisions on some issues but 'less ethical' ones on others.

For reasons that are not entirely clear, other than the general imbalance between the sexes in the IS community, very few (12%) of our respondents were female so it has not been possible to draw any meaningful distinctions between responses on the basis of gender. There is clearly scope for further work in this area.

4. Recommendations

The findings of the survey point to a high level of ethical awareness among those IS professionals who responded. At the same time, there are a number of areas where more guidance and support for individuals is desirable, to encourage consistently responsible behaviour. The following recommendations for organisations, for professional societies and for educators were made as an outcome of this work (Prior et al., 1999):

- It is recommended that organisations should
- promote awareness among all employees of:
 - ethical issues;
 - the organisation's Code of Conduct (if there is one);
 - how the organisation's Code of Conduct may be applied to guide ethical decision-making;
 - provide a working environment that encourages ethical practices, supporting employees in resisting the temptation to allow commercial pressures to lead to ethically dubious practices – instead, promoting their ethical stance to their commercial advantage;
 - consider the promotion of ethical awareness among younger IS professionals, including the use of more experienced personnel as mentors;
 - establish 'whistle-blowing' procedures to encourage employees who become aware of unethical practices within the organisation to come forward;
 - introduce a clear policy concerning the use of computing resources by employees for their own activities, and consider allowing their use for selected *non-profit-making* activities as a contribution to the local community or as a legitimate perk for employees;

- review the security of computer-held data with attention to both technical aspects and management aspects affecting potential threats, especially from *internal* sources;
- consider and clarify their policy concerning the re-creation of intellectual property such as a product, program or design by employees when they move to another employer;
- seriously consider adopting a Code of Conduct for all employees;
 - and if adopted, include in the Code of Conduct provision for full consultation with employees before initiatives such as electronic surveillance are introduced, and ensure that safeguards for employees are put into place.

It is recommended that professional societies representing the IS field should:

- ensure that any Code of Conduct remains up-to-date and relevant to the profession, promoting awareness of the Code among members and providing guidance about how it can be applied in practice;
- provide particular support for their younger members, helping them to acquire greater awareness of the ethical issues they will encounter throughout their careers;
- promote debate of the continuing applicability of legislation such as the software licensing laws, in the light of current developments, opinions and practice.

Professional societies could, for example, promote mentoring schemes for new members, organise training sessions and workshops and produce appropriate literature to help meet the latter two recommendations.

It is recommended that those responsible for the education of future IS professionals should:

- address ethical issues more extensively in their curriculum, to raise the awareness of young, aspiring professionals concerning all of the issues covered in this survey.

5. Conclusion

As shown above, the findings of the survey lead to a number of recommendations. However, there are some limitations to this study and several areas can be highlighted where further investigation is required.

The survey has not attempted to discover the factors influencing the ethical attitudes or the decision-making of respondents. Ford and Richardson (1994) note that there has been little research conducted in this area, although it was discussed by Ferrell and Gresham (1985), Trevino (1986), Bommer et al. (1987), Jones (1991), Pearson et al. (1996) and Banerjee et al. (1998). Neither have we attempted to define what is meant by ‘ethical’; for example we have left it to respondents to use their own definition of an ‘ethical’ project. Banerjee et al. (1998) noted that the value orientation of IS personnel differed from culture to culture, with both inter-country and

intra-country differences existing. However, there have been very few cross-cultural studies of the ethical attitudes of IS professionals; one example being Kumar and Bjorn-Andersen (1990) who investigated the difference between the values of Canadian and Danish systems designers.

There are two main directions in which the survey is being followed up. Firstly, it is being conducted by colleagues in a number of other countries, including Costa Rica, Australia, the United States and Japan. It is hoped that this will enable some cross-cultural comparisons to be undertaken. Secondly, the survey will continue to be undertaken in the UK at two-yearly intervals, with the sponsorship of the IMIS, enabling the acquisition of some longitudinal data.

IS professionals hold positions of considerable responsibility, given the ubiquitous nature of information and communication technologies in the modern world. The value in determining their ethical attitudes lies in the ability to highlight areas of possible contention, where policies may be needed to encourage more ethical behaviour in the workplace and high standards of practice for the profession. This survey has provided some indication of what these policies might be. As part of an ongoing longitudinal project which includes international comparison, it offers the opportunity to ethically ground IS practice of the future.

Acknowledgements

This research was commissioned by the Institute for the Management of Information Systems as part of their strategy to encourage ethical behaviour in the profession.

Appendix A

Respondents were asked to circle the answer representing the extent to which they agreed or disagreed with the statements; responses are given in percentages.

Statement	Strongly disagree	Disagree	Indifferent	Agree	Strongly agree
1 It is acceptable for me to make unauthorised copies of commercial software to use at work	56.5	33.5	3.5	5.3	1.2
2 I would refuse to work on a project that I considered to be unethical	3.6	11.3	7.7	51.8	25.6

Table Continued

	Statement	Strongly disagree	Disagree	Indifferent	Agree	Strongly agree
3	Ongoing consultation with representatives of all those affected should occur throughout the information systems development life cycle	1.8	1.8	1.8	40.5	54.0
4	It is acceptable to use my employer's computing facilities for my own <i>non-profit-making</i> activities if this has no adverse effect on my employer	10.7	25.0	15.5	39.9	8.9
5	It is acceptable to use my employer's computing facilities for my own <i>profit-making</i> activities if this has no adverse effect on my employer	46.7	34.3	5.9	10.1	3.0
6	If an organisation has purchased/developed software for use in the office, it is acceptable for employees to make unauthorised copies of this software for use at home	51.8	28.8	8.2	8.8	2.4
7	I think that all organisations should require all employees to abide by a code of professional ethics	2.4	1.8	3.5	41.8	50.6
8	If a project is significantly behind schedule or over budget, it is acceptable to cut down on testing effort	36.1	46.2	3.0	13.0	1.8

Table Continued

	Statement	Strongly disagree	Disagree	Indifferent	Agree	Strongly agree
9	Employees should be allowed to recreate a product/program/design for another organisation if they change jobs and are no longer employed by the organisation who paid them to create it	26.1	20.0	14.5	32.1	7.3
10	It is acceptable for me to use other employees' access codes <i>with</i> their permission to access data normally hidden from me	27.4	32.1	7.1	25.6	7.7
11	It is acceptable for me to use other employees' access codes <i>without</i> their permission to access data normally hidden from me	74	20.1	1.8	1.8	2.4
12	Employees who violate their organisation's code of professional ethics should be appropriately disciplined	1.2	2.4	1.2	54.8	40.5
13	When disagreements arise between development personnel and those affected by the system, it is the project manager who should have the final say	5.6	37.5	10.0	30.6	16.3
14	Employers are entitled to use electronic surveillance to monitor employees' performance without their consent	34.8	34.1	9.1	17.7	4.3
15	Providing a systems development project provides me with an interesting challenge, I do not care about its overall objectives or purpose	27.4	56.1	8.9	3.8	3.8

Table Continued

	Statement	Strongly disagree	Disagree	Indifferent	Agree	Strongly agree
16	It is acceptable for me to make unauthorised copies of commercial software for my own private use	41.9	43.7	6.6	7.8	0.0
17	My organisation's security arrangements are sufficient to ensure that information held on its computer systems is safe from unauthorised access from <i>internal</i> sources	5.6	28.6	6.8	44.1	14.9
18	My organisation's security arrangements are sufficient to ensure that information held on its computer systems is safe from unauthorised access from <i>external</i> sources	2.5	13.7	3.1	50.3	30.4
19	Organisations should develop and administer an ethics awareness programme for all employees	1.8	0.6	11.9	45.8	39.9
20	It is acceptable for a software contractor, provided with a brief specification, to go ahead and develop the system knowing that in the future re-work under another contract will be essential	25.9	40.1	10.5	19.8	3.7
21	Consideration of the overall working environment is not part of the IS professional's responsibility	28.1	62.3	5.4	3.0	1.2

References

- Athey, S., 1993. A comparison of experts' and high tech students' ethical beliefs in computer-related situations. *J. Business Ethics* 12, 359–370.
- Banerjee, D., Cronan, T.P., Jones, T.W., 1998. Modeling IT ethics: a study in situational ethics. *MIS Quart.* 22 (1), 31–60.
- Barnett, J.H., Karson, M.J., 1989. Managers, values and executive decisions: an exploration of the role of gender, career stage, organizational level, function and the importance of ethics, relationships and results in managerial decision-making. *J. Business Ethics* 8, 747–771.
- Bommer, M., Gratto, C., Gravender, J., Tuttle, M., 1987. A behavioral model of ethical and unethical decision making. *J. Business Ethics* 6, 265–280.
- Conger, S., Loch, K.D., Helft, L., 1995. Ethics and information technology use: a factor analysis of attitudes to computer use. *Inform. Systems J.* 5 (3), 161–184.
- Couger, J.D., 1984. Providing norms on ethics to entering employees. *J. Systems Manage.* 35 (2), 40–41.
- Ferrell, O.C., Gresham, L.G., 1985. A contingency framework for understanding ethical decision making in marketing. *J. Marketing* 49, 87–96.
- Ford, R.C., Richardson, W.D., 1994. Ethical decision making: a review of the empirical literature. *J. Business Ethics* 13, 205–221.
- Fowler, F.J., 1993. *Survey Research Methods*, 2nd ed.. Sage Publications, Newbury Park, California.
- Harrington, S.J., 1996. The effect of codes of ethics and personal denial of responsibility on computer abuse and judgments and intentions. *MIS Quart.* 20 (3), 257–278.
- Jones, T.M., 1991. Ethical decision making by individuals in organisations: An issue-contingent model. *Acad. Manage. Rev.* 16 (2), 366–395.
- Kidwell, J.M., Stevens, R.E., Bethke, A.L., 1987. Differences in ethical perceptions between male and female managers: myth or reality?. *J. Business Ethics* 6, 489–493.
- Kreie, J., Cronan, T.P., 1998. How men and women view ethics. *Commun. ACM* 41 (9), 70–76.
- Kumar, K., Bjorn-Andersen, N., 1990. A cross-cultural comparison of IS designer values. *Commun. ACM* 33 (5), 528–538.
- Leventhal, L.M., Instone, K.E., Chilson, D.W., 1992. Another view of computer science ethics: patterns of responses among computer scientists. *J. Systems Software* 17 (1), 49–60.
- Oppenheim, A.N., 1966. *Questionnaire Design and Attitude Measurement*. Heinemann, London.
- Paradice, D.B., 1990. Ethical attitudes of entry-level MIS personnel. *Inform. Manage.* 18, 143–151.
- Parker, D.B., 1979. *Ethical Conflicts in Computer Science and Technology*. AFIPS Press, Reston, VA.
- Parker, D.B., Swope, S., Baker, B., 1990. *Ethical Conflict in Information and Computer Science, Technology and Business*. QED Information Science, Wellesley, MA.
- Pearson, J.M., Crosby, L., Shim, J.P., 1996. Modeling the relative importance of ethical behavior criteria: A simulation of information systems professionals' ethical decisions. *J. Strategic Inform. Systems* 5 (4), 275–291.
- Prior, M., Rogerson, S., Fairweather, N.B., Butler, L., Dixon, S., 1999. *Is IT Ethical? 1998 ETHICOMP Survey of Professional Practice*. IMIS, Sidcup, Kent.
- Trevino, L.K., 1986. Ethical decision making in organisations: a person-situation interactionist model. *Acad. Manage. Rev.* 11 (3), 601–617.
- Vitell, S.J., Davis, D.L., 1990a. Ethical beliefs of MIS professionals: the frequency and opportunity for unethical behavior. *J. Business Ethics* 9, 63–70.
- Vitell, S.J., Davis, D.L., 1990b. The relationship between ethics and job satisfaction: an empirical investigation. *J. Business Ethics* 9, 489–494.