Nature of e-business ethical dilemmas

Sonja Petrovic-Lazarevic and Amrik S. Sohal
Department of Management, Monash University, Caulfield East, Australia

Keywords *Ethics, Information management, Electronic commerce, Organizational culture, Information officers*

Abstract *Electronic business is based on using computers and networks in all aspects of business. This new business concept is developing its own culture, which faces many ethical dilemmas. One is the role of the chief information officer (CIO). As a leader of information technology application in the organisation, the CIO's ethical behaviour influences the ethics of the electronic business culture in the organisation. In electronic business both the chief executive officer (CEO) and the CIO are responsible for the organisational culture. That is, the CIO has capabilities for reasoning, forming values and making information decisions that contributes to creating corporate core values. From an employee's perspective the CIO is treated as the employer. But being employed by the organisation in a similar way to the rest of the employees, the CIO can also be treated as an employee of the organisation. This duality in the role of CIO causes ethical dilemmas that may be solved through establishing ethical codes that are based on existing global ethical codes. Explores the nature of ethical dilemmas related to e-business and proposes possible solutions, drawing on information from case studies of two Australian companies.*

Introduction

Electronic business (e-business) involves business transactions conducted over computer networks and has been of considerable interest to practitioners and researchers primarily because of its influence on both customers and providers of goods and services. More specifically, it is estimated that e-business creates higher customer satisfaction, by providing quicker service, less effort to buy a product or service, and less business cost compared to a business run without the use of information technology (IT) (McLeod and Schell, 2001). Also, as Laudons note, the e-business literature deals with the technical facilities needed to run a business smoothly (Laudon and Laudon, 2000). Both of these approaches to e-business point to changes in the entire vision of a classical understanding of business. These changes may contribute to the creation of specific social consequences for the organisation, affecting both employers and employees. We argue that one of the consequences relates to the organisation's culture.

Each organisation, including e-business organisations, creates its own culture. The organisational culture is based on an overall subjective employee's perception of the organisation through key characteristics that the organisation values (Schein, 1990; O'Reilly *et al.*, 1991). These characteristics are individual initiative, risk tolerance, direction, integration, management support, control, identity, reward system, conflict tolerance, and communication patterns (Robbins, 1989). A review of current literature identifies significant contributions that have been made to the understanding of organisational culture *per se* (Schein, 1990; Fedor and Werther, 1995; Chatman and Jehn, 1994; Schwab, 2000; O'Reilly *et al.*, 1991). However, there has been relatively little

Information Management & Computer Security
Vol. 12 No. 2, 2004
pp. 167-177

0968-5227
DOI 10.1108/09685220410530807

focus on how an e-business organisational culture develops. To be more precise, current e-business literature pays attention mainly to e-business organisational culture through exploration of the ethical issues of monitoring and surveillance of employees and breaching their privacy rights (Biggs, 2000; Nycum, 2000; Tobias, 2000; Schwab, 2000; Weber, 2000; Lewis, 2000; Turban *et al.*, 1999; Miller and Wecker, 2000; Woodbury, 1998; Gupta, 2000).

Elements of an organisational culture are symbols and slogans, stories, rites and ceremonies, values, norms and beliefs (Petrovic-Lazarevic, 2000). Since the organisational ethics relate to guiding beliefs, standards, or ideals about whether certain acts are good or bad in the business of an organisation, they are also dependent on organisational culture. All employees, however, do not necessarily agree upon organisational ethics. Moreover, if organisational ethics involve value judgements, they can have a legal form. For businesses that make use of computers and the Internet, the ethics reflect the ethical values of managers, information specialists, and users. That is, they reflect the ethical values of top managers, which in this case would include the chief executive officer (CEO) and chief information officer (CIO). In other words, top managers impose an ethical culture by establishing an ethics credo and ethics program and by tailoring codes of ethics to their own companies. They are responsible for the organisational culture. This applies particularly to the CIO, who being in charge of IT applications in the organisation, contributes to creating corporate core values.

From an employee's perspective the CIO is treated as the employer. But being employed by the organisation in a similar way to the rest of employees, the CIO can also be treated as a regular employee of the organisation. This duality in the role of CIO can create ethical dilemmas. At present, the most important of these relate to monitoring and surveillance of employees, and the breaching of their privacy rights (Miller and Wecker, 2000). Such dilemmas can have negative consequences for the success of e-business organisations. It seems that a possible way to solve these dilemmas could be through establishing organisational codes of ethics based on codes at the global level (Frenzell, 1999). But the development of organisational codes that specifically address computer technology is not an easy task (Pruzan, 2001). Reasons are two-fold. Firstly, codes might be effective deterrents to unethical behaviour if they are used to guide behaviour and to punish unethical behaviour. This however, is problematic in that a code of ethics, although reflecting the values of an organisation, does not necessarily provide specific explanation of each value. As a consequence, organisational leadership, including the CIO, is able to broadly interpret what constitutes ethical or unethical behaviour. Thus, according to the circumstances, the CIO can argue that some unethical behaviour may be judged as ethical if it helps to ease a process of re-engineering and restructuring that usually threatens jobs. That is, the CIO's differing judgments of actions that are commonly considered unethical can cause confusion in employees' perceptions of the moral codes of the organisation. Secondly, changes in technology are so frequent that it is practically impossible to constantly up-date an organisation's ethical codes to accommodate these changes (Smith, 2000; Woodbury, 1998). This again can cause broad interpretations of what is ethical and what is not in terms of the application of new technology in e-business.

The aim of the paper is to point to possible ways to solve ethical dilemmas in defining the role of the CIO in an e-business organisation. In this respect, the paper is

structured as follows: part one defines the role of the CIO in e-business and part two relates to ethical dilemmas faced by e-business as it struggles today to define the role of the CIO. Notes from two case studies are included as examples for various arguments. Part three proposes possible ways to solve these dilemmas. The paper ends with concluding remarks.

The role of CIO

Current literature defines the role of the CIO in an IT-oriented organisation and an e-business organisation in the following manner: as the head of the department for development and operation of computer information systems, the CIO is responsible for all information systems and technology in the organisation (Nickerson, 2000; Oz, 2000). This includes maintaining the hardware, software, data storage technology, and IT networks (Laudon and Laudon, 2000); integrating information systems, telecommunications, and management systems (Frenzell, 1999); aligning IT with the business strategy and activities related to the Internet and e-business, and providing education to other executives (Wagner and Sanders, 2001).

The CIO works with different groups of people: employees of the organisation, top executives whose confidence the CIO must gain by providing understanding of the business, and finally, external customers. The role of the CIO is to educate employees in order to encourage innovation, and to demonstrate initiative and creativity in pursuing the organisational vision. In this respect, the CIO initiative includes the education of executives about the latest IT issues and their implementation in business. In particular, that relates to aligning IT with business strategy and activities in accordance with the Internet and e-business. In this role, the CIO faces ethical issues relevant to monitoring and surveillance of employees.

By suggesting to top executives what improvements to apply in IT, the CIO can distort information in favour of any side of IT business. Thus, the CIO, acting as an immoral manager, can send to top executives information that is discordant with accepted organisational ethical principles. He/she, as an amoral manager, can also provide information that lacks ethical perception and ethical sensitivity. Alternatively, as a moral manager, the CIO could provide information that conforms to high standards of ethical behaviour (Carroll, 2001). The above points lead to the consideration that when the organisation is restructuring based on the implementation of IT, there is often a possible threat of job loss among employees. It follows that employees may see the CIO as a cause of their threatened positions. This would create resistance to whatever actions the CIO undertakes as a top manager of the IT sector. When things go astray, this resistance makes the CIO's position vulnerable. Hence, in order to avoid being less popular, the CIO may provide misinformation to other executives by hiding the real business situation, and act amorally or immorally.

By providing education, not only to other executives but to staff as well, the CIO has the opportunity to transfer cultural issues to everyday business that is related to computer networks. Consequently, it is expected that the CIO understands organisational culture, specifically when it may not be in favour of IT implementation in a business. According to Gupta (2000), since the CIO, as the highest-ranking information systems executive, has a leading role in introducing new technologies in a business, he/she may ignore the organisational culture if it is causing problems in achieving IT business goals.

One aspect that is worthy of closer examination is the argument that the top-down process of creating the organisational culture at the corporate level leads to a form of mind control over employees. It is possible that the CIO's position, as one of the top managers, contributes to the treatment of employees as helpless, and unable to think morally or to tell right from wrong (Feldman, 2000). More specifically, after joining the corporate culture, employees are faced with the destruction of distinction between resistance and control, and consequently faced with a meaningless environment. We can anticipate that such an understanding of organisational culturism is not based on the view that employees are still able to think in a controllable environment. This makes the whole organisational culturism concept questionable.

Another problem causing the CIO's position to stand on shaky ethical ground links to the CIO dealing with information that cannot be quantified or measured. Outside the organisation, the CIO does not know, or approve of, how company information may be created, used, and discarded. That is, through the Internet an unprecedented volume of information is available to millions of people for display, analysis and printing (Clark, 1999). According to Frenzell (1999), that is another reason why a CIO should not be identified as a firm's executive, but as an employee.

The literature states that CIO turnover is one of the highest among senior executives. At the global level, every year about one in two CIOs move to another organisation (Oz, 2000). This rate is greater than that of top executives in general. In North America, for instance, one in five CIOs move to another organisation (Frenzell, 1999). Such a high turnover can have positive and negative impacts regarding the role of the CIO as one of top managers. First, relatively frequent replacement of CIOs brings new opportunities to the organisation, such as new ways to run information systems department, to introduce latest IT innovations, to monitor and survey employees, and to find ways not to breach workers' privacy rights regarding the use of Internet, e-mail and voice mail. A negative issue relates to the learning process that is critical to every new employee in an organisation, including the CIO. For the CIO this process is even more difficult, since the new employee is in fact one of the executives. Further, since the CIO, as a top information executive, influences the overall organisational culture, he/she contributes to changing the overall subjective employee's perception of the organisation through key characteristics that the organisation values. Frequent changes of organisational culture do not leave enough time for employees to adapt. As a consequence, unethical behaviour may occur. Such behaviour is visible through the use of Internet and e-mail for other than business purposes, as well as breaching the Customers' Privacy Acts by using customers' data for whatever business reason.

In short, according to the literature review, there are different opinions regarding the role of the CIO in organisational culture. These opinions could be grouped as follows. First, the role of the CIO as one of the top executives is important in establishing and implementing organisational culture. Second, the role of the CIO is important in implementing the latest IT into the business, but organisational culture should not be the CIO's responsibility. The third opinion states that the CIO should be treated as every other employee who is not in charge of defining the organisational culture. We believe that such different opinions about the role of the CIO contribute to creating ethical dilemmas that can cause negative consequences to the success of an e-business organisation.

Ethical dilemmas in defining the role of CIO

Every organisational culture, including e-business culture, expresses core values that are shared by a majority of the organisation's members. However, the e-business organisational culture differs from any other organisational culture by the addition of the CIO. Specifically, the CIO is responsible for management support, and monitoring and surveillance in conflict tolerance, and privacy rights, both in conflict tolerance and communication patterns (Petrovic-Lazarevic, 2001).

There is a widespread view that the CIO, as a leader of an organisation, defines the organisation's values and visions (Pierce and Henry, 2000; Gupta, 2000). Additionally, Gupta argues that the CIO also ensures that all governmental and legal regulations are met (Gupta, 2000). But this statement does not necessarily indicate that the CIO accepts or follows organisational ethical codes. It may also be noted that since ethical codes are part of organisational culture, the CIO should influence organisational ethics by leading by example.

Further, depending on the definition of the role of a CIO in e-business, the interpretation gives rise to the following questions: to what extent should the CIO, defined as a leader, let business organisations regulate themselves without being helped by the government? Is it better to regulate the business process as little as possible by official legal rules, or not (Lewis, 2000)?

Company 1 (C1), the first case study for this paper, consulted a solicitor prior to forming their information privacy policies. Furthermore, C1 consult solicitors about any ethical issues that arise concerning employee behaviour. The firm legal grounding of their policies has enabled the company to adequately deal with a claim of unfair dismissal that has occurred without a messy legal battle in court. Thus it could be argued that constructing ethical codes with the help of legal professionals can save a company time and money if a dispute arises.

Since it is increasingly more common and perhaps accepted in modern business to dehumanise the workforce and customers, thus abandoning Kant's categorical imperative of treating humanity as an end and not as a means, one is led to consider whether the CIO's approval and support of monitoring of employees and customers should continue to be treated as unethical at all (Schonsheck, 2000). More fundamentally, one might consider that IT has provided positive changes to the modern workplace by providing safer working conditions, better communication and increased productivity. However, the question still remains: to what extent is IT responsible for the loss of privacy and human dignity in every-day business by creating enormous possibilities by which employees may be monitored? Employers argue that intensified monitoring is justified by high productivity, which benefits both employers and employees. Furthermore, the tension between the right to control information and individual privacy slips into the question of ownership (Moore, 2000). Employers state that they have the right to own information, even if it is related to private issues, since the information was gathered through the IT assets that belong to them (George, 2000).

According to Taylor (2000), when examining privacy issues and individual autonomy, it is important to distinguish between overt and covert privacy invasions. Overt invasions occur if employees are aware that they are being monitored. In this situation, the employees would most likely refrain from non-business-related Web surfing, as they know their Internet activities are being monitored, thus their autonomy

is reduced. Covert invasions occur if employees are unaware of the surveillance. If employees were not aware that they are being monitored, they would arguably feel free to use the Internet in whatever way they choose, so it would seem that no loss of autonomy has occurred. However, employers are still able to affect employees' behaviour by deciding whether to inform them of the surveillance or not. Thus it could be said that covert surveillance still has the potential to undermine autonomy, which is ethically problematic if the argument holds that personal autonomy is intrinsically valuable (Taylor, 2000). This point gives rise to the question of whether the truth of this contention is entirely dependent either on organisational culture, or on an individual's religious background or community norms. If it is a matter of organisational culture, one could say that there are no ethical dilemmas regarding the role of CIO, since he/she creates the organisational culture together with other leaders of the organisation. In addition, if there were an ethical-technical gap in an organisation caused by the general manager's lack of knowledge of computers and IT, the role of the CIO would be to contribute to the improvement of the general manager's knowledge of IT. Also, to be fair to employees, the CIO should discuss with them the ethical dimension of communicating in business today.

On the other hand, if the understanding of the role of CIO in an e-business were such that the CIO is an employee, would she/he accept monitoring of employees and customers as unethical? We are aware that every business has a moral obligation to respect an individual's right to privacy in the form of legitimate requirements such as monitoring the performance of employees. That includes monitoring of e-mails as well. The question is whether e-mail messages ought to be regarded as public communication or not, if sent from the organisational networks. In other words, since computing equipment should only be used for legitimate work-related purposes, is it up to the employer to allow private e-mails and other Internet activities? The answer perhaps would be dependent on whether the employer has the right to read employees' e-mail, subject to what employees in a particular society understand as their privacy rights. C1 practices "passive monitoring" of their employees' net usage. This means that use of the Internet and e-mail is recorded, and the records are available for access by managers, but these records are not usually accessed unless suspicion of misuse of the Internet or e-mails is raised. Ethical issues are dealt with by the general manager and not the CIO, which would indicate that in this case the CIO is regarded as more of an employee than an employer, not having responsibility for the ethical issues that arise out of technology. However, the CIO is responsible for implementing the technology, including the system of surveillance.

When it comes to how much responsibility the CIO has in the allowance of private e-mails and other Internet activities, the duality of being both employer and employee can create problems. Acting as a manager at one stage can conflict with acting as employee at another stage. This can mislead the leadership process towards managing information systems in strategically unplanned ways. As a consequence, the success of the whole business process can be endangered. Finding appropriate solutions to resolving the tension between monitoring of employees in order to make business successful and maintaining employees' privacy does not seem to be an easy task. It is further complicated by the suggestion of employers that monitoring and surveillance are in the interests of the prosperity of the business and should not be relevant to breaching privacy rights. That is, if the business goes well, both employers and employees benefit, no matter how much the employees' privacy rights are violated.

E-business ethical issues affect not only employees but also customers. That is, misuse of customers' data can cause negative effects on the reputation of an organisation and jeopardise its competitive advantage. Here the role of CIO as a manager can be significant in protecting the privacy of its customers and balancing data from customers against company's need for information to run the business successfully. Company 2 (C2), the second case study for this paper, receives critical customer data as part of its business process. Maintaining the privacy of that data is extremely important for its reputation. Access to the data is tailored according to the customer's preference. The high security measures it has in place such as Dual-key encryption of the data and regular system auditing are essential to ensure that its clients' competitors can not access this data. The sensitive data that would be useful to its customers' competitors pertain to new product launches, and this information is often the kind that the customers want to be kept strictly confidential. Thus there are separate data storage areas for both "public" and "private" data. In C2, the role of its CIO is more like a manager, as its CIO, along with other top managers like the CEO and its IT security head, are the only ones who have access to customer data. Still, in order to secure its clients' trust, it employs a collaborative method of setting security levels between its own policy and what its clients dictate.

Threats to privacy involve the use of transactional data, Web-site data, and the Internet. In particular they involve exposure to information, data surveillance, information brokers, identity theft and sharing information in very sensitive fields such as medicine and the environment. In this respect, there are laws that cover Web-site data and the Internet to a certain extent. But still, today, there are no laws against companies sharing the transactional data of their customers. Furthermore, there are no approaches to protecting personal data through government legislation and self-regulation. In the case of C2, it would not be beneficial to the company's competitiveness to jeopardise the security of their customer data. It could be argued that there is no ethical issue here concerning the use of that data, as being a packaging company, information about their client's new products *per se* is not valuable to the running of their company.

However, customer data has many forms, and in some cases it is very valuable to a company. Consumers who participate in the online world are subject to electronic surveillance of their activities, and often a multitude of spam (electronic junk mail) (Macklin, 1999). Through the use of cookies (small text files that a Web site can send to a user's computer to track their activities) and the compiling of customer information into databases, companies which carry out business online are perfecting the techniques of one-on-one marketing (tailoring advertisements to fit patterns of user interest). This raises a number of ethical issues, including privacy, informed consent, and ownership of such information. In fact, one of the major obstacles that online marketing faces is the lack of trust and concerns about privacy felt by consumers (Macklin, 1999). It appears that some specific corporate actions, such as creating specific privacy policies for their customers, are necessary to protect consumer privacy in an online environment (Caudill and Murphy, 2000).

So far, existing e-business ethical codes are related to global ethical codes and codes of professional societies. That indicates that the way to solve the dilemmas of the role of the CIO in e-business is to implement and adjust global ethical codes, and codes of professional societies.

Possible ways to solve dilemmas

Organisational culture is under the influence of national culture. Subsequently, e-business organisational culture should be under the influence of national e-business culture. Looking at Schein's characteristics of national culture, we could recognise the extent to which this is relevant to e-business (Schein, 1990). Accordingly, entrepreneurial activities, leaders of movements, institution builders, and social architects are dependent on the level and type of national economic development (Pierce and Henry, 2000). That is, national economic development influences the likelihood of businesses becoming e-businesses by creating the circumstances that allow the application of this new type of business. In other words, more developed countries are more able to rapidly develop e-businesses, as this development is dependent on IT application, which developed countries are more likely to be able to afford. Less developed countries, however, lack IT applications. This slows the use and operations of e-business at the international level. This global situation leads to a polarity, where at one end, there is a group of countries that have the facilities to further implement and develop e-business (rich countries), and at the other end, countries with no facilities to do this (poor countries). This increases the dependence of poor countries on rich countries, including the acceptance of developed country's codes that are relevant to e-business. Consequently, it could be concluded that developed countries have a moral responsibility to solve e-business ethical dilemmas, in order to provide guidance for poorer countries in the event that they do develop more e-business.

Countries with the highest use of computer technology that inevitably develop an e-business organisational culture have created codes for e-business (Johnson, 1998; Goldsborough, 2000; Woodbury, 1998; Weber, 2000). At present these codes are accepted at the global level. In some countries, at the national level, the government creates laws relating to the implementation of technology. Laws encompass a right to computer access, a right to acquire computer skills, a right to use computer specialists, and a right to influence computer decision making. It appears that these laws mainly reflect known global ethical codes. In terms of information they include the rights to information privacy, accuracy, property and accessibility (Johnson, 1998).

E-business, *per se*, is a global business since it deals with the Internet and World Wide Web. Accordingly, codes of ethics that have been established at the global level seem to fill the gap that exists between e-business organisational culture and national e-business culture. E-business ethics comprise business ethics and computer ethics and are known as cyberethics or information system ethics. In this respect, the Computer Ethics Institute has created the well-known Ten Commandments of Computer Ethics that are applied by many organisations. Subsequently, if the words computer and Internet replace the existing word "computer" in the Ten Commandments of Computer Ethics, then the Ten Commandments of Computer Ethics can be used in e-business (Goldsborough, 2000). Hence the CIO of every e-business organisation should be responsible for the application of these Commandments. The code of ethics that establishes ideals and responsibilities of the e-business profession should protect both customers and professionals. It should improve the profile of the profession by motivating and inspiring practitioners, raising awareness and consciousness of issues and improving quality and consistency. However, since codes of ethics standards are not obligatory, their ethical values are culturally relativistic (Hilton, 2000).

An interesting opinion on an appropriate code of ethics comes from Johnson. He argues that Internet service providers, e-businesses, online services and civic networks, should have a code of ethics, known as netiquette, to serve new users in cyberspace (Laudon and Laudon, 2000). If applied, it would contribute to solving many ethical dilemmas that appear while using computer technology in Web businesses.

Another attempt to construct guidelines to identifying ethical behaviour for both employers and employees of e-business has been made by Computer Professionals for Social Responsibility (CPSR) (Woodbury, 1998). In their opinion, defining what is ethical in terms of the level of e-mail and v-mail monitoring is different from looking at laws and their enforcement. The level of monitoring can be legal and unethical at the same time, or illegal and ethical. That is, laws do not have to fit the definition of ethics. Consequently, CPSR indicates that ethical use must be defined and enforced. If created as a policy, with the contribution of employees, it would become an integral part of the organisation and its ethics. Otherwise, it may impose unexpected effects on employees.

In Weber's opinion, a code of ethics is a sign of a mature profession (Weber, 2000). Hence, The Software Engineering Code of Ethics and Professional Practice, developed by a joint committee of the Association for Computing Machinery and IEEE Computer Society, the Software Engineering Code of Ethics and Professional Practice, indicates the maturity of the software engineering profession. However, this profession, in spite of claiming its maturity, has still unsolved problems of privacy rights erosion. In particular, the Software and Information Industry Association Company argues that privacy rights erosion is inevitable in collecting consumer data. Further, without consumer data, the company cannot develop competitive products and services.

In Nycum's opinion, the use of information can cause not only ethical concerns, but also legal concerns (Nycum, 2000). In this respect e-business organisations should create their own privacy policies that comply with the European Union's Safe Harbor Privacy Provisions.

In our opinion, in defining its ethical codes based on the afore-mentioned existing global ethical codes, each e-business organisation should, first, define the role of CIO. Then it should point to the duality that is eminent in the CIO role, and clarify what is expected from the CIO in terms of organisational culture. In other words, it should be clearly stated whether the CIO contributes to the creation of organisational culture, or accepts it as is stands. Since the CIO turnover is very high, it is likely that as a new employee in an organisation it would be necessary to accept existing organisational culture. Consequently, within some time spent in the organisation, the CIO may contribute to the adjustment, adding or creating of new ethical issues that are applicable to new IT implementation. It is believed that such an approach to creating ethical codes would help solve ethical dilemmas that arise in defining the role of the CIO in e-business.

Conclusions

The CIO is one of the top managers in an organisation that runs e-businesses. Having capabilities for reasoning, forming values and making information decisions, the CIO contributes to creating the corporate values, norms and beliefs of an organisational culture. In the literature today there are different opinions regarding the role of the CIO in organisational culture that have contributed to creating ethical dilemmas in defining the CIO role. The main ethical dilemmas seem to be related to understanding the role of

the CIO as either the employer or the employee, or both. This understanding is particularly important in the monitoring and surveillance of employees and the issue of breaching of employees' privacy rights. The possible ways to solve these dilemmas would be, first, to define organisational ethical codes based on existing global ethical codes and define the role of the CIO. Second, to determine whether the CIO contributes to the creation of organisational culture, or accepts it as it is. That is, since the CIO turnover is very high, a new CIO in an organisation should ideally initially accept existing organisational culture, and perhaps adjust it later on, and add or create new ethical issues that are critical to new IT implementation. It seems that such an approach would facilitate solving dilemmas in defining the role of the CIO in order to contribute to the business success of an e-business organisation.

References

Biggs, M. (2000), "In implementing emerging technology, we may face thorny ethical problems", *InfoWorld*, Vol. 22 No. 42, pp. 106-8.

Carrroll, A.B. (2001), "Models of management morality for the new millennium", *Business Ethics Quarterly*, Vol. 1 No. 2, pp. 365-71.

Caudill, E.M. and Murphy, P.E. (2000), "Consumer online privacy: legal and ethical issues", *Journal of Public Policy & Marketing*, Vol. 19 No. 1, pp. 7-19, UMI's Proquest Direct, available at: http://proquest.umi.com/ (accessed October 26, 1999).

Chatman, J.A. and Jehn, K.A. (1994), "Assessing the relationships between industry characteristics and organizational culture: how different can you be?", *Academy of Management Journal*, Vol. 37, June, pp. 522-53.

Clark, R. (1999), "Ethics and the Internet: the cyberspaces behaviour of people, communities and organisations", *Business and Professional Ethics Journal*, Vol. 18 No. 3-4, pp. 153-67.

Fedor, K. and Werther, W.B. (1995), "Making sense of cultural factors in international alliances", *Organizational Dynamics*, Spring, pp. 33-48.

Feldman, S.P. (2000), "Management ethics without the past: rationalism and individualism in critical organisation theory", *Business Ethics Quarterly*, Vol. 10 No. 3, pp. 623-43.

Frenzell, C.W. (1999), *Management of Information Technology*, Course Technology, Cambridge, MA.

George, R.T. (2000), "Business ethics and the challenge of the information age", *Business Ethics Quarterly*, Vol. 10 No. 1, pp. 63-72.

Goldsborough, R. (2000), "Computer and ethics", *Link-up*, January-February, pp. 9-12.

Gupta, U. (2000), *Information Systems*, Prentice-Hall International, Upper Saddle River, NJ.

Hilton, T. (2000), "Information systems ethics: a practitioner survey", *Journal of Business Ethics*, Vol. 28 No. 4, pp. 279-84.

Johnson, J. (1998), "Netiquette training: whose responsibility?", *CPSR Newsletter*, Vol. 16 No. 3, pp. 14-18.

Laudon, K.C. and Laudon, J.P. (2000), *Essentials of Management Information Systems*, Prentice-Hall, Upper Saddle River, NJ.

Lewis, B. (2000), "No privacy: employers watch every click you make. And what's wrong with that?", *InfoWorld*, Vol. 22 No. 46, pp. 58-60.

McLeod, R. and Schell, G. (2001), *Management Information Systems*, Prentice-Hall International, Upper Saddle River, NJ.

Macklin, B. (1999), "E-commerce at what price? Privacy protection in the 'information economy'", Master's in Legal Studies (Commercial Law), Faculty of Law, Australian National University, Canberra.

Miller, S. and Wecker, J. (2000), "Privacy, the workplace and the Internet", *Journal of Business Ethics*, Vol. 28 No. 3, pp. 256-65.

Moore, A. (2000), "Employee monitoring and computer technology evaluative surveillance v. privacy", *Business Ethics Quarterly*, Vol. 10 No. 3, pp. 697-709.

Nickerson, R.C. (2000), *Business and Information Systems*, Prentice-Hall, London.

Nycum, S. (2000), "Play fair with info on the Web", *InformationWeek*, Vol. 27, November, pp. 192-4.

O'Reilly, C.A. III, Chatman, J. and Caldwell, D.F. (1991), "People and organisational culture: a profile comparison approach to assessing person-organisation fit", *Academy of Management Journal*, Vol. 34 No. 3, pp. 487-516.

Oz, E. (2000), *Management Information Systems*, Course Technology, Singapore.

Petrovic-Lazarevic, S. (2000), "Civil engineering and construction industry: organisational culture in Yugoslavia", in Gyulay, J. (Ed.), *Civil Engineering Management 2000 Monograph*, Az Epites Fejodeseert Alapitvany I Terc Kft, Budapest.

Petrovic-Lazarevic, S. (2001), "Electronic business culture ethical dilemmas", in Callaos, N., Yunfa, H., Rodriguez, M. and Quang, H. (Eds), *Proceedings of World Multiconference on Systemics, Cybernetics and Informatics, SCI 2001*, International Institute of Informatics and Systemics, Orlando, FL, pp. 200-4.

Pierce, M.A. and Henry, J.W. (2000), "Judgements about computer ethics: do individual co-worker, and company judgements differ? Do company codes make a difference?", *Journal of Business Ethics*, 20 December, pp. 307-22.

Pruzan, P. (2001), "The questions of organizational consciousness: can organizations have values and visions?", *Journal of Business Ethics*, Vol. 29 No. 3, pp. 271-81.

Robbins, S. (1989), *Organisational Behavior*, Prentice-Hall, Upper Saddle River, NJ.

Schein, E.H. (1990), *Organisational Culture and Leadership*, Jossey-Bass, San Francisco, CA.

Schonsheck, J. (2000), "Business friends: Aristotle, Kant and other management theorists on the practice of networking", *Business Ethics Quarterly*, Vol. 10 No. 4, pp. 897-910.

Schwab, A.J. (2000), "Applied ethics: a third-millennium approach", *IEEE Spectrum*, November, pp. 23-6.

Smith, C. (2000), "The ethical workplace", *Association Management*, June, pp. 70-3.

Taylor, J.S. (2000), "Big business as big brother: is employee privacy necessary for a human-centered management organisation?", *Business and Professional Ethics Journal*, Vol. 19 No. 3/4, pp. 13-28.

Tobias, Z. (2000), "Putting the ethics in e-business", *Computerworld*, Vol. 34 No. 45, pp. 81-5.

Turban, E., McLean, E. and Wetherbe, J. (1999), *Information Technology for Management*, John Wiley & Sons, New York, NY.

Wagner, S.C. and Sanders, G.L. (2001), "Considerations in ethical decision making and software piracy", *Journal of Business Ethics*, Vol. 29 No. 1/2, pp. 161-7.

Weber, A. (2000), "Ethics? Not interested", *Software Development*, Vol. 8 No. 5, pp. 7-9.

Woodbury, M. (1998), "E-mail, voicemail, and privacy: what policy is ethical?", available at: www.cpsr.org/-marsha-w/emailpol.html