
Communications of the Association for Information Systems

Volume 3, Article 8
April 2000

PROFESSIONAL ETHICS IN INFORMATION SYSTEMS: A PERSONAL PERSPECTIVE

Robert M. Davison
Dept of Information Systems
City University of Hong Kong

isrobert@is.cityu.edu.hk

PROFESSIONAL

PROFESSIONAL ETHICS IN INFORMATION SYSTEMS: A PERSONAL PERSPECTIVE

Robert M. Davison
Dept of Information Systems
City University of Hong Kong

isrobert@is.cityu.edu.hk

ABSTRACT

In the Information Systems discipline, increasing attention is being paid to the issue of professional ethics. In this article, a personal perspective on the topic is offered. The academic philosophies of ethical theory are introduced, followed by detailed treatment of four fundamental issues: codes of ethics, intellectual property rights, professional accountability and data protection. The intention of the article is to arouse the interest of IS professionals and to stimulate debate. Through a discussion, future developments in the professionalism of information systems are explored, and questions are raised concerning the way in which information systems is regulated, and the role it may play in the future.

Keywords: Professional ethics, codes of ethics, data privacy, intellectual property rights, professional accountability.

I. INTRODUCTION

The purpose of this article is to encourage the Information Systems (IS) community to consider and debate professional ethics. While the article has been informed by and developed from the Professional Ethics pages of ISWORLD - it is also a personal perspective. Various other equally legitimate perspectives – such as those of government, business, industry, and independent regulators, are not presented to a significant extent.

Ethics as a discipline of study and practice is by no means new, with historical antecedents dating to the philosophy of Confucius and Aristotle, and its application to computers to the work of mathematician/philosopher, Norbert Wiener [Wiener, 1950]. However, this article focuses primarily on the ethical issues of relevance to IS professionals - in academia, industry and the public sector. In this context, the term “professionals” is defined very broadly, and includes not only academics, practitioners, researchers, executives and consultants, but also students, since many graduating students will become professionals in due course. Geographically and culturally, the article is not limited to any particular norms, and does attempt to compare "Western" notions of ethics with norms that are prevalent in “non-Western” cultures.

Ethics has been defined as involving the systematic application of moral rules, standards, or principles to concrete problems [Lewis, 1985; Martinsons & So, 2000], though the utilitarian nature of this definition is criticised by some [e.g. Snell, 1996] who would also pay attention to the characters (and obligations) of the key actors. In general, it is agreed that an "ethical dilemma emerges whenever a decision or an action has the potential to impair or enhance the well-being of an individual or a group of people" [Martinsons and So, 2000]. Naturally, such decisions or actions are undertaken frequently, with competing values or conflicts of interest all too common in the information society. Various philosophical perspectives can be applied to the tackling of ethical dilemmas, including utilitarianism, deontology and social propriety.

Numerous books have been published in recent years on the general topic of “Ethics and Information Technology”, e.g. Baase [1997], Johnson and Nissenbaum [1995], Spinello [1995]. Such books offer broad introductions to the field, typically including: a background to the academic philosophies of ethics and a framework to help analyse ethical dilemmas, together with chapters on specific ethical issues. Many books also include teaching cases for student analysis. Some books restrict themselves to more specific topics, e.g., Langford’s [2000] “Internet Ethics” and Floridi’s [1999] “Philosophy and Computing”. All of these books investigate ethics in far more detail than this article and are strongly recommended.

In addition to relevant books, an extensive literature in professional ethics exists in academic and professional journals, some focusing exclusively on IT ethics (e.g. Ethics and Information Technology), others examining ethics within business (e.g. Journal of Business Ethics), or behavioural (e.g. “Ethics and Behavior”) contexts. Some journals (e.g. Communications of the ACM) occasionally devote special issues to ethical topics (e.g. the February 1999 issue on Internet Privacy), while others publish occasional articles with an ethical flavour. Journal articles that introduce some fundamental issues include: Cappel and Kappelman [1998]; Kock [1999]; Laudon, [1996]; Mason, [1986]; Myers and Miller [1996]; Weisband and Reinig [1995]. A parallel literature examines the development of ethical values by individuals. Key contributors to this literature include Kohlberg [1976, 1981], and more recently Snell [1995, 1996, 1999].

The key ethical issues that emerge from these various sources include: (1) codes of ethics; (2) intellectual property rights (IPR); (3) data (and personal) privacy, particularly with respect to the Internet and applications such as email; and (4) professional accountability. Other issues include electronic monitoring of employees [Sipior and Ward, 1995; Weisband and Reinig, 1995]; computer security (including hacking and unauthorised access) [Hoffer and Straub, 1989; Straub and Nance, 1988; Straub and Welke, 1998] and IT law (particularly software contracts, agreements and liabilities, and actions that involve the fraudulent use of computers)[Lee, 1995].

In this article, we introduce and discuss some of the fundamental issues in the professional ethics of information systems, namely, codes of ethics, IPR, accountability and data protection. Whilst the legal and security issues are interesting, they are also complex and hence are generally beyond the scope of the article.

II. ACADEMIC PHILOSOPHIES OF ETHICS

A variety of formal and informal principles and guidelines have been suggested as means to assist in the resolution of ethical dilemmas. These include Deontology, Teleology, Altruism, Egoism and the Christian 'Golden Rule'[1].

Teleology, etymologically derived from the Greek '*telos*' meaning 'end' or 'goal' involves valuing goals or ends that are 'good'. A correct decision would maximise the good for most people. Utilitarianism, developed by Bentham (1748-1832) and Mill (1806-1873) is one example of a teleological theory, involving an analysis of the 'goodness' of consequences. One must note, however, that goodness should not apply only to the individual making the decision, but also to all parties that are affected by the decision. As Velasquez [1992] notes, however, the principle of utilitarianism "assumes that all benefits and costs of an action can be measured on a common numerical scale and then added or subtracted from each other". This calculation of costs and benefits is inherent in utilitarianism, and some form of cost-benefit analysis will apply to most teleological theories. Naturally, it is impossible to be certain of all the possible consequences of an action. Therefore, one can never be certain that the right action is being taken. However, this uncertainty can be moderated by making a decision based upon "the best possible knowledge of the consequences available at the time" [Walsham, 1996, p.71]. A second concern with teleology is that on occasion the methods used may be inherently evil, though the end result may be deemed beneficial for the majority: witness the killing of civilian demonstrators to protect the stability/sovereignty of a nation state. Since the goal itself may be

subjectively perceived, the methods to achieve the goal may necessarily be equally subjective.

Contrasting with teleology, deontology (Greek '*deon*' meaning 'obligation' or ‘duty’) focuses on the duties that individuals (or entities such as organisations or society) have in particular situations. The correct decision to make does not depend on an outcome, but on a set of fundamental duties (e.g. the Bible’s Ten Commandments). Walsham [1996, p.70] observes that deontological theories “are based on the view that there are certain sorts of acts that are wrong in themselves, and thus they are morally unacceptable, even if the ends which are being pursued are morally admirable”. Kant (1724-1804) focuses on the *duty* of the individual, irrespective of any notion of happiness or satisfaction. Indeed, according to Kant, one *must* act according to one's duty - irrespective of what the consequences might be. Kant's concept of duty is often referred to as the categorical imperative - an ultimate test of whether something is right or wrong. Universalism is implicit in this principle - only if an action can be performed by everyone can it be morally acceptable. If everyone pirated software, then no one would buy it, no one would spend resources developing it, and it would not even exist; therefore, no one should pirate software. The categorical imperative "can be reduced to the absolute principle of respect for other human beings, who deserve respect because of their rationality and freedom, the hallmark of personhood for Kant" [Spinello, 1995, p.25].

The categorical imperative is a good principle, but it is too perfect! There are often situations where there may be conflicting duties and the consideration of consequences is necessary in order to reach an optimal (or ‘least worst’) decision, for example sending spam email to identify a possible bone marrow donor for a life-saving operation. Indeed, some moral philosophers do recommend that a combined teleological-deontological code of ethics be adopted [Hunt and Vitell, 1986].

Duties are often associated with corresponding rights - and humans are sometimes more interested in their rights than their duties. These rights, however, “are not universally accepted, and can be held to be strongly

conditioned by particular cultures" [Walsham, 1996, p.71]. This conditioning has become apparent in recent years with conflicts about the universality of so-called "Western" values (rights) and their applicability in some developing nations, notably those in South East Asia.

The universality of an action is often analysed by what we know as the Golden Rule - broadly: 'Treat other people in the same way that you would like them to treat you'. It can be helpful to turn the tables, make oneself the victim or recipient of an action - and then decide if the action is acceptable or not. Other, less formal, tests that can be used are sometimes called the TV, Market and Mum tests. Could you publicise your action on TV? Could your behaviour be used as a marketing tool? What would your Mum say? Such tests start to move away from the universal principles that we have been discussing towards relativism - presumably not all mothers will think in the same way or respect the same goals or duties. Likewise, TV audiences in different cultural contexts may apply somewhat different ethical principles to evaluate the 'goodness' or 'rightness' of a decision, perhaps because of different social values or standards.

III. CODES OF ETHICS

Codes of ethics, which amount to a formalisation of rules and expected behaviours, are tied up with many of the ethical issues in Section II. We should make it clear at the outset that Information Systems, unlike Law or Medicine, is not a controlled profession. In most countries, in order for a lawyer or medical doctor to practice, membership of a professional association is required - and adherence to the ethical code of that association is obligatory. Violation of the code may lead to various penalties - suspension of membership, and hence of the right to practice, or more serious consequences such as judicial investigation and imprisonment.

Many information systems professionals belong to professional associations and are expected to adhere to their codes of ethics, but we are not aware of any employing organisations that mandate membership of such a professional association as a condition of employment/practice. Nevertheless,

codes of ethics are valuable as they both raise awareness of ethical issues and dilemmas that professionals may potentially face and also serve to enhance the public profile of the profession. Furthermore, codes of ethics may provide clarifications about the conduct deemed acceptable in client-professional relationships.

However, codes of ethics have their drawbacks. Promoting a particular set of beliefs brings a natural tendency to universalise what kind of ethical behaviour is acceptable, despite evidence to the contrary. For example, it is apparent that social and ethical values vary in different cultural contexts, informed by different social, educational and political norms. It would surely be arrogant to impose ethical values, developed in one culture, on another culture, all the while assuming that what is good for one person (or society) must be good for another. If true, then the same imposition should work in reverse.

Codes of ethics, under one name or another, abound. In information systems, relevant codes of ethics have been developed by many professional associations (Table 1). These codes vary in their complexity and degree of 'bindingness'.

Table 1. Sample Professional Associations in IS

ACM	Association for Computing Machinery	CSSA	Computer Society of South Africa
ACS	Australian Computer Society	HKCS	Hong Kong Computer Society
BCS	British Computer Society	IEEE	Institute for Electrical and Electronic Engineers
CIPS	Canadian Information Processing Society	SCS	Singapore Computer Society

The ACS, for example, comments:

> "…an essential characteristic of a profession is the need for its members to abide by a Code of Ethics. The Society requires its members to subscribe to a set of values and ideals which uphold and advance the honour, dignity and effectiveness of the profession of information technology" [ACS, 2000].

The ACS code forms part of a larger set of regulations, and violation of the code may lead to the expulsion of a member.

One of the most comprehensive professional codes has been developed by the BCS, having separate codes of conduct and practice, as well as professional development. The code of conduct is split into four areas covering a member's duties with respect to: public interest; employers and clients; the profession; and professional competence and integrity. The code of practice comprises "a series of statements which prescribe minimum standards of practice, to be observed by all members" [BCS, 2000a]. With respect to professional development, the BCS maintains "to maximise your potential for life time employability, it is essential that you maintain high levels of professional competence by continually upgrading your skills and knowledge" [BCS, 2000b]. It is not feasible in this article to explore this, and other codes of ethics, conduct or practice, in greater detail. However, readers are directed towards the excellent materials freely available on the web pages (see the ISWORLD pages on professional ethics for current URLs), as well as towards Oz's [1992] article comparing five codes of ethics and Walsham's [1996] article that uses ethical theory to critique the ACM code of ethics.

IV. INTELLECTUAL PROPERTY RIGHTS

Intellectual Property Rights (IPR) concern the protection of all products created or designed by the human intellect - books, songs, poems, trademarks, blueprints … and software. Where professional ethics are concerned, it is primarily the protection, or violation of that protection, of software programs that is probably of greatest concern - at least to the software developers. In this section, we discuss some of the legal background to IPR and the justification for protecting copyright, drawing upon codes of ethics to supplement the explanations. We then consider some cultural differences that complicate the notion of copyright, and finally consider the rights and duties of software developers and software users. While we seek to investigate IPR in a manner conducive to the development of professional ethics, we are nonetheless aware of the danger of upholding a set of values that is distinctly biased towards the

software industry, and is in consequence perhaps not so professional. We will return to this debate both in the following section – on professional accountability – and in the discussion in Section VII.

The copying of software programs, although nominally protected by copyright laws, is certainly widespread. While some may acknowledge that such copying is tantamount to theft, the activity persists if only because it is so easy, the chance of getting caught is considered negligible, and the software developers are perceived as quite rich enough already. Such copying is not restricted to personal users – businesses are involved as well, though often inadvertently. As the Business Software Alliance [BSA, 1999a] reports:

> "employees contribute significantly to the presence of illegal software in the workplace, posing serious financial and legal consequences for their employers. Among those [companies] surveyed, software decision-makers indicate that colleagues bringing software from home (40%), downloading unauthorized copies from the Internet (24%), and sharing programs with other employees (24%) are three of the most common violations occurring at their companies".

Since 1994, the BSA, in conjunction with the Software Information Industry Association (SIIA) has conducted annual surveys of software piracy. In 1998 (the latest year for which figures are available), the survey:

> "estimates that, of the 615 million new business software applications installed worldwide … 231 million - or 38% - were pirated. This represents an increase of 2.5 million more applications than were pirated in 1997" [IPR, 1999; BSA, 1999b].

Countries where software piracy is estimated to be most prevalent include Vietnam (97%) and the PRC (95%). The USA (25%) and UK (29%) are the only countries with rates below 30%.

One philosophical basis for software protection lies in the *prima facie* right to private property, particularly property that can be said to be the 'fruit of one's endeavours' [Locke, 1964]. Naturally, such a right is characteristic of those

capitalist societies that legislate the protection of individual rights, though copyright laws protect the *expression* of ideas (a software program, for instance), but not the idea itself. In Chinese society however, for instance, the "socialization process emphasises obligations and duties that promote conformity, collective solidarity, and obedience while downplaying assertiveness and creativity" [Martinsons and So, 2000]. Bond and Hwang [1986] note succinctly the similarity between a "preoccupation with social order" in Chinese society and a "preoccupation with individual freedom" in Western societies. These fundamental cultural and social differences certainly raise difficulties in legislative attempts to provide for universal protection of creativity.

A danger inherent in copyright protection is that when a technology is wholly owned by a single entity (individual, organisation), consumers may be harmed because the opportunity for competition is much diminished. Monopolies can lead to reduced evolution and diffusion of products, as well as overpricing and underproduction. Given these opposing forces, there clearly needs to be a reasonable balance between protection of a product on the one hand, and the right of consumers to avail themselves of the product at reasonable cost on the other. Indeed, in Korea and Japan there is a public assumption that new ideas and technologies should be shared in the public domain so that members of a society can benefit [Spinello, 1995, pp.161-162]. In those countries with a Confucian heritage, notably the People's Republic of China, Wingrove [1995] remarks: "the copying of works of almost any kind has for centuries been regarded as honourable and necessary". Swinyard [1990], confirms this view, observing that "in many Asian nations the highest compliment one can be paid is to be copied". In many developing countries, meanwhile, governments are, quite naturally, more concerned that new technology should spread through all of a society as rapidly as possible, enabling the country to leapfrog older generations of technology and catch up with the rest of the world[2]. The notion that technology should in some way be strongly protected, with profits going overseas, is not one that they feel is good for the development of the local economy. In such contexts,

"individual claims on intellectual property are subordinated to more fundamental claims of social well-being" [Steidlmeier, 1993].

Much of the argument about IPR lies in the deontological dichotomy between rights and duties. Software producers claim that they have the right to protect the fruit of their endeavours - the software programs. Furthermore, they have the right to be compensated for the resources that they have expended in the development of that product. This right is translated into a right to charge consumers what they deem a fair price for the software products - a price that covers the various developmental costs, as well as generating profits that can be used for future product research and development. To protect their right to the fruit of their endeavours, they claim that consumers have a duty both to pay the price and to respect the intellectual property contained within the product - by not stealing it.

Notwithstanding these rights and duties, consumers may claim that they have the right to use a product for which they have paid, and indeed have the right to expect that that product will be free of defects (bugs). This imposes a duty of quality (and professionalism) on the developers of the software to ensure that the software is indeed bug-free. Consumers expect that a product be competitively priced, providing value for money.

V. PROFESSIONAL ACCOUNTABILITY

Professional accountability is an issue that is closely tied to many codes of ethical conduct. For example, in the BCS code of conduct, clause 21 reads: “Members shall accept professional responsibility for their work and for the work of their subordinates and associates under their direction, and shall not terminate any assignment except for good reason and on reasonable notice” [BCS, 2000c], and in the BCS code of practice, clause 2.4 requires members to: “be accountable for the quality, timeliness and use of resources in the work for which he/she is responsible” [BCS, 2000a]. In general, accountability lies at the root of vendor-client relationships, and is therefore relevant to our professional

behaviour in consulting or professional work, especially with those who make use of our products or advice.

Accountability is important because it shows that high-quality work is valued, encourages professionals to be diligent and responsible in their practice, and establishes just foundations for punishment and/or compensation when software does not perform according to expectations, or when professional advice turns out to be unreliable. Accountability is also important because computer software is used throughout our society, and is an essential component of many life-critical systems, such as transportation equipment (aircraft, trains, lifts), medical devices, toys, accounting and financial control systems (ATMs), weapons systems, communications devices (radar, telephones, televisions, satellites, networks), and domestic appliances (microwave ovens, TVs, refrigerators, air-conditioning systems).

Through encouraging a strong sense of professional accountability, we can attempt to ensure that those who are responsible for the safe functioning of these systems will do their utmost to ensure that systems are safe, and will minimise risks. Accountability runs a considerable risk of being eroded, however, when computers are made scapegoats for human failings or when developers of computer software deny any responsibility for the consequences of use of the software, even when this use is in accordance with the purpose for which the software was designed. Johnson and Mulvey [1995, p.59] use a scenario to illustrate an accountability dilemma of this type. A computerised investment system has been designed for and purchased by a pension fund management company. The user of the system becomes familiar with it, and requests IT staff (not the original designer) to make some modifications to the system. Shortly afterwards, substantial losses are incurred and payments to pensioners have to be cut. Who is accountable? The original system designer? The user who requested modifications? It is perhaps all too easy to blame the computer, apologise, and do nothing.

Accountability is generally assumed to include a number of components, viz.: responsibility (direct or indirect), liability and strict liability. Responsibility can

be determined if a person either performed (or failed to perform) an action [causal condition], or intended to perform an action [mental condition]. It may not be possible to identify a single responsible person - particularly for the causal condition. Liability relates to who should pay compensation (financial redress, community service,…) as a result of being held responsible for an action. In some situations, strict liability may apply, i.e. requiring the payment of compensation to a victim even though the harm has not arisen through one's deliberate or direct actions. An example might relate to aircraft systems. If an aircraft crashes due to a system failure, then the airline is subject to strict liability even though the airline has not deliberately or directly caused the crash. Strict liability helps to ensure that extraordinary care is taken over the development and maintenance of systems that have the potential to cause loss of life.

Although the definition of accountability is fairly straightforward, four barriers to accountability can be identified: the problem of too many hands; the computer as scapegoat; the problem of bugs; and ownership without liability. Computer software is especially vulnerable to the problem of too many hands, because most (if not all) software is necessarily designed and developed by a number of individuals, often at different points in time. Furthermore, software often has a symbiotic relationship with computer hardware. This makes it very difficult to identify precisely which person should take responsibility for any unexpected action. However, such complexity can be no defence and there is a clear need to attempt to identify who should take responsibility for the problem. If we do not attempt to apportion blame, not only will the responsible person(s) escape blame, but they may cause further problems to happen in the future. The net result is that accountability is eroded, with no one prepared to step forwards and take responsibility.

Information systems are often blamed for human errors because they intermediate communications between people. If a human action is mediated by a computer, there is a strong tendency to blame the computer rather than the human (designer, programmer or user) that caused the computer to produce incorrect information. It is expected that with the forthcoming ‘webalisation’ of

domestic devices (kettles, microwave ovens, air conditioning systems, etc.), computers will be made scapegoats for human failings with increasing frequency. In this situation, it is vital to establish lines of responsibility because it is all too easy for humans to shirk their responsibilities.

Bugs include all types of software errors, including those made at the design, modelling and coding stages of system design. Bugs certainly make software unreliable and can cause system failure, with the potential for loss of life or severe damages. There has been an unfortunate tendency for bugs to be seen as an inevitable aspect of computer systems, even natural hazards that computer users have come to accept. This view is not restricted to the software developers, with prominent commentators on IT ethics voicing similar views, Spinello [1995, p.91] asserting “It is the nature of software programs to have errors…”. However, the very purpose of professional accountability is that we should identify who has caused a harm to occur - whether intentionally or through negligence. If, playing the Devil’s advocate, we accept that bugs are inevitable, then accountability becomes impossible - we can merely regret that harm was caused, but defend ourselves by saying that bugs are unavoidable (even expected) and therefore no one should be held responsible for the harm. There may even be resistance to liability - if no one can be identified as accountable, then why should anyone pay compensation - which is precisely why the concept of strict liability is so important. If, however, we do not view bugs as natural hazards, but as manifestations of unprofessional and sloppy work, we should be able to identify lines of responsibility, particularly for persistent bugs. Furthermore, if we are to act as true professionals, we cannot be satisfied with the notion that bugs are inevitable - it is like saying that the loss of human life through human error is inevitable, and that when we turn on a TV set, there is a reasonable chance it will short circuit and electrocute us. Society has the right to expect that domestic appliances, and many other essential systems, will function safely.

As we have mentioned previously, the legal aspects of software product reliability are complex. Nevertheless, in order to understand the relationship

between bugs and liability, it is instructive to introduce the legal rights and duties of developers and customers. Strict liability is generally only applied by courts when a person or property is injured or damaged. Thus, purely economic damages are usually held to be beyond the application of strict liability. A second category of liability is known as negligence. Developers can avoid accusations of negligence by ensuring that they take reasonable care in the design, coding and testing of their products. One problem here relates to the thoroughness of testing. If a company has followed industry standards with regard to testing, then it would appear that if bugs still exist, it cannot be accused of including such bugs either deliberately or through carelessness [Spinello, 1995]. Whilst this does not obviate the requirement for software to be bug-free, it certainly does imply that industry standards may need to be set at very high levels. A third liability category is known as breach of warranty. A warranty is essentially a promise that the developer makes to the customer with regard to the functionality of the software, and forms “part of the contractual agreement between the seller and the buyer” [Spinello, 1995, p.87].

Having identified these categories of liability, it is important to note that pre-packaged softwares (Microsoft Word, Netscape Navigator, etc.) are generally recognised to be *products*, but custom-developed applications are considered to be *services*. This distinction is critical since while the standards of liability are applicable to products, they are not to services. Individually customised software must therefore be legally covered by the specific contract that is agreed upon between the developer and the customer, where penalties for non-functionality, lateness of delivery, etc. may be specified.

Computer software developers affirm that they sell a user the licence to install and use (typically) a single copy of a software package; they are not selling the ownership of the software. However, at the same time, software developers employ disclaimers to minimise as far as possible any liability (e.g. for financial or data losses) arising out of the customer's use of the software. Indeed, we note an unfortunate tendency for software producers to deny to the maximum extent possible any responsibility for actions caused by their software. At the

same time, consumers are held to be liable for any use of the software that lies outside the narrowly-worded terms of the software license agreement. This situation has the effect of eroding the rights of the user, since virtually all the risks of using the software (but few of the rights) are transferred to the user. Legally, these disclaimers have been recognised in courts so long as they are explicit and prominently displayed. There is evidence to indicate that the tendency to disclaim liability is growing more serious, Menn [2000] noting that many software companies intend to implement measures that would have the effect of further diminishing consumers' rights.

Another consequence of minimising liability is the software developers' parallel denial of responsibility for any bugs that they may include (intentionally or inadvertently) in the software. Essentially, when you buy software, you install and use it "as is", i.e. at your own risk. We argue, however, that such transfer of risk is unreasonable because it imposes upon the developer no duty to ensure that software is bug-free, nor even - so long as these bugs do not cause loss of life or injury - to provide bug-fixes when they are identified. This seems to be both unethical and unprofessional - consumers have the right to use a product that fulfils the agreement with the vendor - explicitly or implicitly. At the same time, developers have a moral duty to ensure that the software they sell is usable and "fulfills the explicit and implicit contract between the buyer and seller" [Spinello, 1995, p.89]. We maintain that if software developers wish to retain their ownership rights, then they should be both responsible and liable for their products, since they are in the best position (owning source code) to have direct control over the quality of their software.

We suggest that accountability and liability to compensate need to be separate. An individual programmer or software designer may be responsible for a harm, but liability more properly lies with the employer, since it retains responsibility/ownership for the work of its employees. There is a strong need to clarify and promote standards of care in system design that are acceptable to users and developers alike - perhaps via a code of practice. Furthermore, the practice of extensive disclaiming needs to be reviewed. At the very least,

customers have the right to be informed if there are known bugs, irrespective of whether the developer intends to fix them, and irrespective of whether the developer thinks they are significant or not. Not informing the customer amounts to misrepresentation. Indeed, misrepresentation can be a form of contract violation and so may potentially attract legal penalties of a different kind. With respect to bugs, appropriate standards of testing need to be promulgated and adhered to, while excellent documentation of "who does what" should enable lines of accountability to be established. Independent software auditors may be called upon to verify software quality, if possible applying ISO standards.

Accountability is clearly vital not only for the information systems profession, but also for us as professionals, if we are to be held in the highest regard by those for whom we develop systems.

VI. DATA PRIVACY

Privacy, “the right to be let alone” [Warren and Brandeis, 1890], is one of the most contentious issues of the information age, one that is fraught with ethical complications. The capability of information systems to gather, process, sort, store and distribute all forms of information is unparalleled in human history, and as a direct consequence, the confidentiality of this information has been severely eroded. In place of confidentiality has come commercialisation - that is, all forms of information can be bought and sold - for a price. Given the commercialisation of information, personal privacy has directly suffered, with little attention being paid to the rights of individuals, despite laws that aim to protect personal privacy.

Data about individuals is collected in a wide variety of ways, including information provided on application forms, credit/debit card transactions, and web-site transactions (including cookies). This information can then be recombined and reprocessed, before being sold selectively to whoever is interested. A good example of such data reprocessing and selective distribution is the Lotus *Marketplace: Households* software developed (and quickly withdrawn) by the US firms Lotus Development Corporation and Equifax for

distribution in 1991. The product, to be delivered on CD-ROM, drew upon a database of 80 million US households, including: name, address, gender, marital status, income level and shopping habits. Businesses would be able to buy a minimum of 5,000 names worth of data - data relevant to their own line of business, for example the names and addresses of single males between 30 and 40 years of age living in Southern California and with an annual income exceeding $200,000 who have bought sports cars in the last 3 years.

This type of database marketing system (DMS) has become the lifeblood of many small and medium sized enterprises (SMEs) that need to locate their customers with direct mailing (or emailing) campaigns. If such DMSs became unavailable, one could argue that many jobs in SMEs risk disappearing. Nevertheless, we must also ensure that the privacy of individuals is protected - and that individuals consent to the use of their information. It is sensible to assume that most individuals are concerned about their personal information and wish to keep it confidential. This is particularly true for the more sensitive forms of information - financial and medical, for example.

Nevertheless, individuals (data subjects) are routinely asked if they would permit their information to be used by the information collector (more properly the data user). Application forms invariably include a clause stating that personal information provided may be used (unless the individual requests to the contrary) for marketing or other purposes. This is the principle of informed consent - if the individual does not so request that his/her data not be used for those other purposes, it is assumed that permission has been given. The alternative principle, of affirmative consent, where an individual is required to give permission for each and every occasion on which a data user wishes to make use of an individual's data, becomes prohibitively expensive and logistically complex (in terms of managing the permissions of many individuals), and is consequently seldom practiced [Spinello, 1995].

Although these principles provide some internal regulation of the individual's privacy, many countries have developed data privacy legislation with varying degrees of protection. Legislation was typically enacted to protect the

ever increasing amount of data held on computers, much of it unknown to the data subjects, as well as data transferred between organisations – nationally and internationally (known as trans-border data flows). The first of these laws that specifically addressed the issue of computer-based information appeared in Europe in the early 1980s, though only after EEC pressure [Langford, 1995] e.g. the 1984 Data Protection Act in the UK [Moulton, 1989; Wong, 1994]. A more recent, and very comprehensive example of a data protection law, is that enacted in the Special Autonomous Region of Hong Kong in the People's Republic of China. This key provisions of this legislation, enacted in December 1996, are introduced briefly as they provide a comprehensive view of the data protection possibilities.

In 1996, the Hong Kong Government enacted the data privacy ordinance and set up the Office of the Privacy Commissioner for Personal Data (PCO). This office has many responsibilities, including promoting awareness of the ordinance, approving codes of practice relating to implementation, investigating suspected breaches of the ordinance and issuing enforcement notices to data users as appropriate. The ordinance [PCO, 2000a], which is designed to protect the privacy interests of living individuals in relation to personal data, comprises six data protection principles, viz.:

- Purpose and manner of collection - data should be collected in a fair and lawful manner. Data users should explain to data subjects what data is being collected and how it will be used;
- Accuracy and duration of retention - personal data that has been collected should be kept accurate, up-to-date, and for no longer than is necessary;
- Use - data must only be used for the specific or directly-related purpose for which it was collected. Any other use is conditional on consent of the data subject;
- Security - suitable security measures should be applied to personal data;
- Information availability - data users should be open about the kind of data that they store and what they use it for;

- Access - data subjects have the right to access their personal data, to verify its accuracy, and to request correction.

Certain classes of data are exempted from the ordinance, including: data held for recreational or domestic purposes (a personal address and telephone number list, for example); certain employment related data may be exempted from subject access (e.g. performance assessments); subject access and use limitation exemptions may be provided for data considered to be prejudicial to the public interest, including: security, defence, international relations, the prevention and detection of crime, and assessment of taxes. The web pages of the PCO provide considerably more detail than can be given here, including the complete ordinance and examples of situations where the PCO was requested to investigate suspected breaches of the ordinance.

The data privacy ordinance is primarily protective of the rights of individual data subjects, who have the right to check "whether their personal data are held, to obtain a copy of such data, and to have personal data corrected" [PCO, 2000b]. A direct consequence of the enactment of the ordinance is that all organisations that keep personal data in Hong Kong need to ensure that they follow the six data protection principles. This necessarily includes the appointment of a data protection officer who is charged with registering with the PCO the nature and details of data held by the organisation. The data protection officer must ensure that data users (and other people with access to personal data) are appropriately trained in security measures designed to prevent loss, damage or inappropriate disclosure of data, while also establishing procedures through which data subjects can apply for access to their data.

Bearing in mind the need that some SMEs have for DMSs, and hence arguments that such data needs to be as fluid as possible, we can identify several challenges to data protection legislation. First, it is very difficult to prove that an organisation has data, since it requires the cooperation of the organisation both to reveal that it has information, and to reveal how much information it possesses. Although the law specifies penalties for non-disclosure, one can imagine that if all organisations refused to disclose the contents of their

databases, it would be impractical for judicial authorities (most likely the police, with their limited resources and expertise in this domain) to mount detailed investigations of all their databases. This kind of limitation has lead to the PCO being labelled a toothless tiger - it has laws at its disposal, but it is constrained in the extent to which it can use those laws to investigated suspected transgressors. With respect to junk electronic mail (spam) (email addresses being commonly available by the million on CD ROM), the PCO advises that one should first request (if possible in writing) the sender to desist spamming, thereby exercising one's right to 'opt out'. If the spamming continues, one may refer the case to the PCO – who, one suspects, may have great difficulty tracing the source of the junk mail given the tendency to disguise identities. In practice, such email spamming is very difficult to prevent, the more so as emails advertising the existence of CDs with millions of email addresses use those same CDs to spam - and need only a very low response rate (1% would be 10,000 responses in a million) to justify the few dollars expended on the CD in the first place.

Electronic commerce is a case in point where data privacy is concerned (particularly for the business-to-customer component), since e-com firms both need to contact their potential customers (spamming seems a logical, if unprofessional option), and need to collect personal data - names, addresses and credit card information - in addition to the buying habits that customers demonstrate through their use of their web sites. Such data can usefully be recombined and further distributed to agencies that specialise in data collection and dissemination, even though such data recombination is likely to be illegal - at least in those jurisdictions that maintain data privacy legislation. Laudon [1996] suggested a solution to the thorny 'control of private data' problem that incorporates what he terms a 'National Information Marketplace'. Essentially, any individual can sell (as frequently as s/he likes) his/her information through an information banking system to information buyers – who can do more or less whatever they like with it - subject to legal constraints. Laudon points out that this approach has the merit of giving some control back to individuals who can set the price of buying their information. Furthermore, by centralising the exchange of

information, information users have to be registered with a licensing authority that must possess some regulatory power and hence ensure that there is no wholesale misuse of information provided in this way, perhaps also acting as a conduit for complaints about data use. Such an information exchange might alleviate some of the legal restrictions that prevent data use by those organisations most dependent upon it. At the same time, if an individual chooses not to sell his/her information (at any price), protection should be guaranteed and it would then be much easier to follow up any case of privacy violation, though one suspects that given the current litigious climate in North America, there would be fodder for lawyers for years to come.

One final challenge to privacy relates to what Roger Clarke [1999a] termed dataveillance: “the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons”, sometimes also referred to as electronic monitoring. Dataveillance can take the form of video monitoring, telephone monitoring, web-site tracking, speed of data entry for typists or lines of code generation for programmers, and email content surveillance. See Clarke [1999b] for a detailed introduction and analysis of the relevant issues in dataveillance, as well as extensive references and hyperlinks to other relevant work.

VII. DISCUSSION

Professional ethics is a contentious topic for an article, since understandably few people like to be told either how to think or what to do! In the preceding pages, we presented some of the arguments relating to four types of ethical issues – codes of conduct/practice, intellectual property rights, professional accountability and data privacy. Given the acknowledged differences in IT application between nations and cultures [Martinsons and Westwood, 1997], we do not believe that the international IS community will be able to agree upon a comprehensive ethical code that will apply to all IS professionals in all countries - despite the increasing communicative proximity engendered by the so-called ‘global village’. Although the codes of ethics

developed by several major professional associations, e.g. the ACM, CIPS, ACS, BCS, are reasonably similar and would not cause much disagreement, there is much in our work that is not currently codified or legislated. Furthermore, cultural differences, while perhaps not so apparent between Europe and North America, certainly are apparent when one considers the social and cultural values that exist on the Western side of the Pacific Ocean. Such countries cannot be quietly dismissed and ignored - not only do they have an important role to play in world economic development, but this role is increasing in importance with most South East Asian economies now beginning to bounce back after the financial crises of the late 1990s.

There are arguments to the effect that these developing or recently developed countries are merely following patterns of economic development that occurred in Europe and North America, and so it is consequently inevitable that political and social patterns will change in due course. This view seems to be an ethno-centric (and perhaps politico-centric) - one that assumes that the Western model of economic development is the only effective one - and that social and professional values associated with that model are more or less uniform: when you follow the road, the values come along as part of the package. Such arguments neglect several millennia of independent cultural and social development, and are naïve in their assumption that culture can be shaped by external economic forces. Even a cursory reading of Hofstede's [e.g. 1987, 1988, 1991] analyses of cultural differences should reveal sufficient variation to suggest that societies do develop in different ways, and that principles relevant in one culture may not be relevant in another.

Nevertheless, such economic rationalisations do not seem to help us very much in an analysis of professional ethics, as they focus on hypothetical norms rather than on what is actually the central issue - "do professional ethics really matter, and what can we do about it?". Most commentators would assert that professional ethics are very important - if for disparate reasons - and many have made attempts to unify the standards that they believe should apply. Oz [1992,

p.432], for instance, suggests that the IS profession should adopt a unified code which is “free of obligations to any specific country” and represents “an obligation to mankind”. This is laudable, though one suspects that some countries would see such a unified code as a form of attack on their national sovereignty or interference with their domestic affairs. Oz [1992, p.433] also suggests that “an ethics code without sanctions is a crocodile without teeth”. This is certainly true, but leads to the suggestion that perhaps the IS profession should become, like Law and Medicine, a controlled profession, where membership of a suitably accredited national (or international) association is a requirement of practice. Such a change in the nature of the profession might lead to much higher standards of ethics, if only on a local/regional basis, since failure to observe those ethical standards might lead to the loss of one’s right to work, quite apart from any other legal charges.

An alternative perspective on this debate emerges if we consider, at least rhetorically, what is going to happen if we don’t tighten up our ethical standards. There is a distinct possibility that professional ethics will be hijacked by the key profit-making organisations in our industry - the hardware and software developers and consultancies - who will then seek to ensure, almost certainly through legislative means, that their rights (as they define them) are protected, and probably that their duties are minimised. Dan Couger predicted such legislative tightening a decade ago when he wrote “unless professionals improve their ethical practices, legislation will force them to do so” [Couger, 1989, p.211]. Indeed, the shift from industrial to post industrial/post capitalist/informational society, predicted by Daniel Bell almost three decades ago [Bell, 1973], and echoed by Peter Drucker [1993], is noteworthy for the implicit suggestion that the source of power will lie ever more effectively with those who create and manipulate information. The extent to which corporations can control information flow is perhaps alarming. Lenzer and Shook [1998] demonstrate how when an employee leaves one company to take another job, the work that s/he does is constrained - under the guise of protecting confidential information to which the former employee has had access and which s/he may not divulge. This kind of

information control seems paradoxical in an economy supposed to thrive on freedom of information. The resemblance with the centralised methods of control practiced in supposedly controlled economies and closed societies, such as that of the People's Republic of China, bears further investigation. As Scollon [1998] remarks, "while 'Western' corporations are globalizing trade practices, they are in turn being globalized by adopting 'Chinese' practices of information control" and "are actively constructing a dynastic world information system within the global corporation".

If the purpose of having professional ethics is to promote the quality of goods, services and knowledge, and perhaps hopefully also contribute to the well-being of society, then is that societal prosperity best guaranteed by ethical standards protective of an individual person's (or corporate person's) creativity, or those that are protective of a powerful (and perhaps corporate) elite's ownership and control of state-of-the-art knowledge? It seems that there is a clear danger of the nation-state and its legal framework being supplanted by a new hegemony - the globalising, corporate body - which claims rights and protection for its products and knowledge, promoting ethical values that correspond to its standards (irrespective of national or cultural boundaries, since operations are increasingly transnational), while at the same time controlling what we know, and what we do (or are allowed to do) with what we know.

VIII. CONCLUSION

Over-all, there is a critical need for heightened debate on professional ethics in Information Systems. Although many professional associations developed codes of conduct, these associations have limited powers – even if a member is suspended or expelled, this cannot be a strong sanction so long as, when considering wider employment issues, membership of a professional association is optional. Changing the status of the IS profession to bring it into line with the legal and medical professions might at least have the benefit of giving such codes more teeth, and hence more respect. At the same time, it does

not seem that an international code or association (at least on a mandatory basis) is an appropriate solution given the wide cultural variations that exist. Nevertheless, that cultural diversity is no reason to prevent us from encouraging local and regional associations to develop their own codes and standards for local enforcement. All codes evolve over time, and will influence one another.

Some readers may find the suspicions about corporate entities having considerable say in a new world order too far-fetched for serious attention. Be that as it may, it is likely that these corporate entities will at least attempt to flex their legal(istic) muscles, defining for themselves what they believe their rights to comprise, and what our duties are. This much they are already doing. There is no knowing how much they may continue to do so, and we should, at minimum, be watchful. It does not seem that the best interests of our society (now almost wholly dependent on information systems) will be served if we keep quiet and kowtow to the masters of the new world order. As academics and practitioners, but above all as professionals, we have an obligation of responsibility towards our various clients: students, consumers, customers and society. Given that responsibility, it does seem necessary that we act to maintain our professional independence, regulate our professional culture in a manner of our choosing and identify the ethical values to which we aspire through codes of professional ethics that are appropriate for our various cultures, times, places, and spaces.

END NOTES

[1] A Confucian version of the Golden Rule is characterised by Martinsons and So [2000] as "do *not* do unto others that which you would *not* want done to you".
[2] For an introduction to, and further information on, leapfrogging, see Davison et al. [2000].

Editor's note: This article was received on March 2, 2000 and was published on April 3, 2000.

ACKNOWLEDGEMENTS

The author wishes to thank Duncan Langford, Maris Martinsons and Doug Vogel for helpful comments made on earlier drafts of this article.

REFERENCES

EDITOR'S NOTE: The following reference list (as well as the text) contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that
1. these links existed as of 3-4-00 but are not guaranteed to be working thereafter.
2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.
4. the author of this article, not CAIS, is responsible for the accuracy of the URL and version information

ACS (2000) "Australian Computer Society Code of Ethics", http://www.acs.org.au/national/pospaper/acs131.htm.

Baase, S. (1997) *A Gift of Fire: Social, Legal and Ethical Issues in Computing*, Englewood Cliffs, NJ: Prentice Hall.

BCS (2000a) "British Computer Society Code of Practice", http://www.bcs.org.uk/aboutbcs/cop.htm.

BCS (2000b) "British Computer Society Continuous Professional Development", http://www.bcs.org.uk/cpd/part1.htm.

BCS (2000c) "British Computer Society Code of Conduct", http://www.bcs.org.uk/aboutbcs/coc.htm.

Bell, D. (1973) *The Coming of Post-Industrial Society*, New York: Basic Books.

Bond, M.H. and K.K. Hwang (1986) "The Social Psychology of Chinese People", in Bond, M.H. (ed.) *The Psychology of the Chinese People,* Hong Kong: Oxford University Press.

BSA (1999a) "Business Software Alliance, Press Release: 'Employer Beware… National Survey Cites Employees as Significant Contributors to Software Piracy in the Workplace'"

http://www.bsa.org/pressbox/enforcement/937503928.html,September 16.

BSA (1999b) "Business Software Alliance, Press Release: 'Worldwide Business Software Piracy Losses Estimated at Nearly $11 Billion in 1998'", http://www.bsa.org/pressbox/enforcement/927637266.html, May 25th.

Cappel, J.J. and L. Kappelman (1998) "The Year 2000 Problem and Ethical Responsibility: A Call to Action", *The Information Society*, (14)3, pp. 187-197.

Clarke, R. (1999a) "Roger Clarke's Dataveillance and Information Privacy Pages", http://www.anu.edu.au/people/Roger.Clarke/DV/.

Clarke, R. (1999b) "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

Couger, J.D. (1989) "Preparing IS Students to Deal with Ethical Issues", *Management Information Systems Quarterly*, (13)2, pp. 211-216.

Davison, R.M. et al. (2000) "Technology Leapfrogging in Developing Countries: An Inevitable Luxury?", *Electronic Journal of Information Systems in Developing Countries*, 1(5) http://www.unimas.my/fit/roger/EJISDC/vol1/v1d5.pdf.

Drucker, P.F. (1993) *Post-Capitalist Society*, Oxford: Butterworth-Heinemann.

Floridi, L. (1999) *Philosophy and Computing*, London: Routledge.

Hoffer, J.A. and D.W. Straub (1989) "The 9 to 5 Underground: Are You Policing Computer Crimes", *Sloan Management Review*, (30)4, pp. 35-43.

Hofstede, G. (1987) "The Applicability of McGregor's Theories in South East Asia", *Journal of Management Development*, (6)3, pp. 9-18.

Hofstede, G. and M.H. Bond (1988) "The Confucius Connection: From Cultural Roots to Economic Growth", *Organizational Dynamics*, (16)4, pp. 4-21.

Hofstede, G. (1991) *Cultures and Organisations: Software of the Mind*, New York: McGraw Hill.

Hunt, S.D. and S. Vitell (1986) "A General Theory of Marketing Ethics", *Journal of Macromarketing*, (6)1, pp. 5-16.

IPR (1999) "International Planning and Research Study for the Business Software Alliance and the Software Information Industry Association: 1998 Global Software Piracy Report", http://www.bsa.org/statistics/GSPR98/98ipr.pdf

Johnson, D.G. and J.M. Mulvey (1995) "Accountability and Computer Decision Systems", *Communications of the ACM*, (38)12, pp. 58-64.

Johnson, D.G. and H. Nissenbaum (1995) *Computers, Ethics and Social Values*, Englewood Cliffs, NJ: Prentice Hall.

Kock, N.F. (1999) "A Case of Academic Plagiarism", *Communications of the ACM*, (42)7, pp. 96-104.

Kohlberg, L. (1976) "Moral Stages and Moralization: The Cognitive Development Approach", in Lickona, T. (ed.) *Moral Development and Behavior: Theory, Research and Social Issues*, New York: Holt, Rinehart and Winston, pp. 31-53.

Kohlberg, L. (1981) *Essays on Moral Development, Volume One: The Philosophy of Moral Development*, San Francisco: Harper and Row.

Langford, D. (1995) *Practical Computer Ethics*, London: McGraw Hill.

Langford, D. (ed.) (2000) *Internet Ethics*, London: Macmillan.

Laudon, K.C. (1996) "Markets and Privacy", *Communications of the ACM*, (39)9, pp. 92-104.

Lee, M.K.O. (1995) "Legal Control of Computer Crime in Hong Kong", *Information Management and Computer Security*, (3)2, pp. 13-19.

Lenzer, R. and C. Shook (1998) "Whose Rolodex is it Anyway?" *Forbes*, (161)4, pp. 100-104.

Lewis, P.V. (1985) "Defining Business Ethics: Like Nailing Jello to the Wall", *Journal of Business Ethics*, (4)5, pp. 377-383.

Locke, J. (1964) *Second Treatise of Civil Government*, New York: Bobbs-Merrill.

Martinsons, M.G. and S.K.K. So (2000) “The Information Ethics of American and Chinese Managers”, Pacific Rim Institute for Studies of Management Report 2000-02.

Martinsons, M.G. and R.I. Westwood (1997) “Management Information Systems in the Chinese Business Culture: An Explanatory Theory”, *Information and Management*, (32)5, pp. 215-228.

Mason, R.O. (1986) “Four Ethical Issues of the Information Age”, *Management Information Systems Quarterly*, (10)1, pp. 5-12.

Menn, J. (February 4, 2000) “Software Makers Aim to Dilute Consumer Rights”, *Los Angeles Times,* http://www.latimes.com/business/updates/lat_rights000204.htm.

Moulton, S. (1989) “The UK Data Protection Act 1984”, *Journal of Information Science Principles and Practice*, (15)1, pp. 55-56.

Myers, M.D. and L. Miller (1996) “Ethical Dilemmas in the Use of Information Technology: An Aristotelian Perspective”, *Ethics and Behavior*, (6)2, pp. 153-160.

Oz, E. (1992) “Ethical Standards for Information Systems Professionals: A Case for a Unified Code”, *Management Information Systems Quarterly*, (16)4, pp. 423-433.

Oz, E. (1993) “Ethical Standards for Computer Professionals: A Comparative Analysis of Four Major Codes”, *Journal of Business Ethics*, (12)9, pp. 709-726.

PCO (2000a) Office of the Privacy Commissioner for Personal Data, “Personal Data (Privacy) Ordinance”, http://www.pco.org.hk/ord/index.html.

PCO (2000b) Office of the Privacy Commissioner for Personal Data, “Implications for Data Users and Data Subjects”, http://www.pco.org.hk/ord/index.html#imp.

Scollon, R. (1998) “Globalism and the New World Order: Person, Property and Power in Intertextuality”, Paper presented at the *Annual Meeting of the American Anthropological Association, Philadelphia*, December 2-6.

Sipior, J.C. and Ward, B.T. (1995) “The Ethical and Legal Quandary of Email Privacy”, Communications of the ACM, 38(12), pp. 48-54

Snell, R.S. (1995) “Does Lower Stage Ethical Reasoning Emerge in More Familiar Contexts?”, *Journal of Business Ethics*, (14)12, pp. 959-976.

Snell, R.S. (1996). “Complementing Kohlberg: Mapping the Ethical Reasoning Used by Managers for their Own Dilemma Cases”, *Human Relations*, (49)1, pp. 23-49.

Snell, R.S. (1999) “Obedience to Authority and Ethical Dilemmas in Hong Kong Companies”, *Business Ethics Quarterly*, (9)3, pp. 507-526.

Spinello, R.A. (1995) *Ethical Aspects of Information Technology*, Englewood Cliffs, NJ: Prentice Hall.

Steidlmeier, P. (1993) “The Moral Legitimacy of Intellectual Property Claims: American Business and Developing Country Perspectives”, *Journal of Business Ethics*, (12)2, pp. 157-164.

Straub, D.W. and W.D. Nance (1988) “Uncovering and Disciplining Computer Abuse: Organizational Responses and Options”, *The Information Age*, (10)3, pp. 151-156.

Straub, D.W. and R.J. Welke (1998) “Coping with Systems Risk: Security Planning Models for Management Decision Making”, *Management Information Systems Quarterly*, (22)4, pp. 441-469.

Swinyard, W.R., H. Rinne and A.K. Kau (1990) “The Morality of Software Piracy: A Cross-Cultural Analysis”, *Journal of Business Ethics*, (9), pp. 655-664.

Velasquez, M. (1992) *Business Ethics: Concepts and Cases* (3rd Ed.), Englewood Cliffs, NJ: Prentice Hall.

Walsham, G. (1996) “Ethical Theory, Codes of Ethics and IS Practice”, *Information Systems Journal*, (6)1, pp. 69-81.

Warren, S.D. and L.D. Brandeis (1890) “The Right to Privacy”, *Harvard Law Review*, (193), pp. 193-220.

Weisband, S.P. and B.A. Reinig (1995) “Managing User Perceptions of Email Privacy”, *Communications of the ACM*, (38)12, pp. 40-47.

Wiener, N. (1950) *The Human Use of Human Beings*, London: Eyre and Spottiswoode.

Wingrove, N. (1995) "China Traditions Oppose War on IP Piracy", *Research-Technology Management*, (38)3, pp. 6-7.

Wong, E.Y.W. (1994) "Data Protection Legislation in Hong Kong - A Practical Perspective", *Journal of Information Technology Management*, (5)3, pp. 59-63.

ABOUT THE AUTHOR

Robert M. Davison is Assistant Professor in the Department of Information Systems at the City University of Hong Kong. His current research interests involve an examination of the impact of Information Systems on group decision making, communication and learning, particularly in cross-cultural and developing country settings. He is co-page manager of ISWORLD's Professional Ethics and Global IT pages. His work has been published by *Information and Management, the Information Systems Journal, Communications of the ACM and Decision Support Systems.*

Communications of the Association for Information Systems