Verizon Visiting Professorship in Business Ethics and Information Technology

A lecture on March 22, 1999 by:

Dr. Richard T. De George
University Distinguished Professor of Philosophy
and Business Administration,
Director of the International Center for Ethics in Business at the
University of Kansas

Speech

It is an honor to have been chosen the first Bell Atlantic Visiting Professor in Business Ethics, and it is a pleasure to be here to inaugurate the Professorship. Bentley has always been in the forefront of business ethics. The Bentley Center for Business Ethics was one of the first established in the world. As the home of the Corporate Ethics Officers Association, it continues its pioneering work. And it is now leading us into the new millennium. Where business ethics is heading, as signified by this new program--what the next stage of business ethics should be--is the topic of my remarks today.

The fact that we are entering the Information Age is a truism, yet exactly what that means is understood differently by different people.

The extent to which we have entered the Information Age is hinted at by the Y2K phenomenon. Correcting the Y2K problem will cost more than $600 billion dollars worldwide. This shows the extent to which business has integrated and become dependent on computer technology. We shall come to realize on January 1, 2000, all the little places date sensitive information has entered our lives in ways that we have forgotten.

As we enter this new Age, we will face new ethical and business issues. This evening I shall briefly present some thoughts about theses issues in seven theses that I hope we can pursue in questions and comments from you in the interactive portion of this presentation.

Thesis I. The IT head in the sand syndrome: Many businesses fail to realize either that we have entered the Information Age or fail to appreciate its importance.

The move of business to the Information Age raises many ethical issues but has received little ethical attention, either from business or from business ethicists. Uncovering the ethical issues that grow out of Information Technology, facing them, and providing ethical guidelines is the major challenge for business and business ethics at the start of the new millennium.

The rise of the Internet as a locus of business is changing marketing, for instance. It makes possible one on one marketing by tracking the customer, recording his or her preferences and

proclivities, and presenting the customer with products he or she is more likely than not to want to buy. Department stores and discount stores, just like TV ads, have to rely on generalizations and average wants and desires. The Internet makes possible an individual fit. As Internet sales climb, they will continue to encroach on, if not yet threaten, department stores and other stores and retail outlets. Many businesses seem not to care or worry, or else do not know how to respond effectively.

Wal-Mart is one of the few traditional firms that realizes it is in the Information Age. In a real sense Wal-Mart is not primarily in the retail business but in the information business, very much like Amazon.com, except that Wal-Mart also owns its own outlets. For, like Amazon.com, Wal-Mart's database is probably its most important asset. Because of it, Wal-Mart can customize each of its stores to suit local shoppers and order product to point of delivery at exactly when each store needs it, saving storage and other costs and changing the way product is manufactured and delivered. The effect of this time pressure on factories and workers in those plants that supply Wal-Mart, however, is uncharted territory for the business ethicist. The changes are real. But their ethical impact has yet to be assessed. The security of Internet transactions, the return of goods with which customers are dissatisfied, and the delivery of goods ordered all raise issues to be examined, and carry with them ethical implications. Similarly, how, where, and whether to tax on-line sellers and buyers is an unresolved question that has been temporarily put on hold by legislation. But the tax base of many cities and local communities relies on local sales taxes, which may well diminish considerably as new ways of buying goods develop in the Information Age. Business via the Internet changes the relevance of location, geography, times during which businesses are open and employees work, how employees are used, and so on. In area after area businesses have not yet started to sort out the implications and society has not decided whose laws should apply, what rules and regulations should be adopted, who is to decide, and who is to enforce them. The pirating of software, music, books and anything that can be put in digital form is symptomatic of a growing nest of problems. The failure of business to recognize the move into the Information Age is demonstrated by its procrastination in facing up to the Y2K Problem. That information technology and computer people could not get the attention of management long before the approach of the year 2000 to fix a problem the technicians knew existed and would have to be faced sooner or later is a sad reflection on business managers. Undoubtedly, many did not understand the problem or its scope, and many who did were unwilling to spend the millions of dollars it would take to fix their systems before they had to, even though the delay added to the cost. Companies are now backing into the Information Age or being pulled by a technology they do not completely understand, even as they become more and more dependent on it. One result is the focus of my second thesis.

Thesis II: The abdication of IT ethical responsibility: The Myth of Amoral Computing and Information Technology permeates the public as well as the business mind, implicitly accepts the technological imperative, and undermines business ethical responsibility.

The lack of awareness of the ethical implications of the Information Age I call the Myth of Amoral Computing and Information Technology. The Myth says that computers are not good or bad, information systems are not good or bad, they simply have a logic and rationale of their own. To speak of ethics with respect to them is to make a category mistake. Hence, when the computer is down, that is no one's fault. When programs malfunction or software has bugs, that

is no one's fault. In general anything that has to do with computers and information technology has a life of its own and is not susceptible to moral evaluation or blame or censure.

This myth is understandable in part because so few people in or out of business truly understand computing and information technology. They are tools that we non-techies like to have and use. But we do not take ethical responsibility for them, and because of our ignorance we do not expect anyone else to take ethical responsibility for them. The result is a failure both to accept and to assign responsibility.

In businesses in the more developed countries, management for the most part still tends to think of Information Systems and Information Technology as something that is not central to the organization. Most managers do not understand them, and tend to ignore them. AI and IT offices are not typically center stage at corporate headquarters, and the typical manager is not a computer techie. The disconnect between corporate leaders and their technical divisions, which are still often off in a back set of rooms and considered part of the support structure and not part of the core business is the clearest indication that firms have not moved consciously into the Information Age. Yet if we are truly in a developing Information Age, then IS and IT need to be at the center of things, and management has to both understand them and take responsibility for them.

The phenomenon of the Y2K problem to which I referred is symptomatic of the Myth of Amoral Computing and Information Technology. We all know the Y2K problem, and we know that law firms throughout the US, probably throughout the world, are gearing up to handle suits and to defend companies against suits for damages as a result of companies failing to solve their Y2K problems in time. Yet amidst all the publicity, there is scarcely any mention of any moral blame or discussion of the moral dimensions of the problem. It is as if computer programmers are not responsible for not fixing programs earlier or managers are not responsible for making sure their products are Y2K compliant or firms are not responsible for fixing their Y2K problems before they reached crisis proportions. The failure of any moral discussion is almost unbelievable, considering the general concern with business ethics in so many other areas.

Thesis III. Where are the business ethicists when you need them?: The task of the business ethicist in the present period of transition--and a task in which few are engaged--is to help anticipate the developments and ease the transition by not losing sight of the effects on people.

The transition is from the Industrial Age to the Information Age. The ethical issues in business of the Industrial Age are those with which we are familiar. The development of the Information Age came about without conscious direction. As technology developed the transition came along as a handmaiden. One consequence is that businesses and society as a whole are following the technological imperative--what can be developed is developed and implemented. Because the transition to the Information Age is currently taking place, many of the ethical issues have not clearly jelled. The task of the business ethicist in this instance is to at least keep up with the technological and social developments and identify problems and potential problems before they cause great harm and before they become embedded ways of doing business, such that they are difficult to change.

Business ethicists and society in general could wait for ethical problems and injustices of the Information Age to arise, and do our analysis after the fact. Far preferable, however, is to anticipate injustice, prevent it from appearing, form structures that are ethically justifiable, rather than having to undo and attempt to reform structures that are unfair, socially disruptive and harmful to some of the parties. We of course cannot anticipate all the ethical issues that will arise, and experience and the empirical approach are also necessary. But we can anticipate more than we might expect, and I suggest that now is the time to start this analysis as we enter the Information Age. We do not need a new ethics, but we have to apply and possibly revise our ethical concepts and norms to fit the new environment. We need an imaginative analysis of the potential harms to people-be they in the realm of privacy, of property, of the new surveillance sweatshops, or of other areas.

Thesis IV. Surmounting the Information Nexus: In order to lay out the ethical issues of the Information Age in business, we need to give careful attention to an analysis of the concept of information and the related concepts with which it forms a whole.

We can start by a simple analysis of information to see the virtues and the vices basic to it. A second step is to superimpose the analysis of information upon the analysis of industrialization to see how it changes production, exchange, advertising, conditions of employment, ownership rights, and so on. Each of these is transformed in the Information Age and the transformation requires new thinking about its effect on people.

If by information we mean not simply data but useful data, we see immediately that what we are interested in is useful information. Information, as generally used, stands for true knowledge in some area. Its opposites are disinformation, misinformation, and falsehood. Information is not simply data but data that represents reality. It is true and not false. Two virtues appear immediately. One is truth (and so truthfulness), the other is accuracy. It follows that the virtues necessary for the Information Age are not necessarily the same virtues as are or were necessary for the Industrial Age. In the latter efficiency became paramount. As opposed to an agricultural age, punctuality became important and time took on critical importance. In the Information Age truthfulness and accuracy take on special importance. For if the information is not accurate or truthful or correct, it is worse than useless. It is dysfunctional. It is ironic that in our society in which truthfulness no longer seems to hold a place of honor, and in which we find people, including high government officials, lying, truthfulness takes on more importance than ever.

False information is injurious to a system built on information. So we have truth as a necessary virtue and a presupposition, and distortion of the truth, lying, the spreading of false information as vices to be guarded against. It is not only necessary for people not to lie or deceive or mislead, but it is also necessary to represent reality as accurately as possible. The enemy of accuracy is inaccuracy, which also leads to disinformation and error. These two virtues or values are basic to any system of information if it is to be socially useful and economically valuable for business as well as for societies and the individuals within them.

Questions that immediately arise are: information of what or of whom and for what or for whom? Information about the world or scientific information is one kind of information; information about societies or social information is another kind; information about people and

corporations is another kind. Important to all of them in an Information Age is ownership, and together with ownership goes power, and with it the dangers of control and manipulation. Truth leads to the concepts of enlightenment, education and the potential freeing of individuals and of society. As individuals learn the truth, they are also in a position of empowerment. Politically this makes enslavement difficult and it promotes self-rule or democracy. Nonetheless, there remains the possibility of the domination of citizens by government and of employees by employers, as well as of one society by another, for instance through the domination of the communication resources.

Ethics is about people and their relations, and it is with this aspect of information that we can also get some inkling of problems and potential pitfalls of which we should be wary. The computer, so prominent in the Information Age, has the capacity to change our concept of ourselves and of others--our concept of what it is to be human. Computers as tools can free human beings to be truly human; or if they become the models against which we measure humanity, they can dominate our thinking and lead us to see ourselves as computers, storers and manipulators of information, and as thinking machines or robots, devoid of dignity and freedom.

Information about individuals clearly raises the issue of privacy, and information about corporations leads to the comparable problems associated with trade secrecy and espionage. As information becomes a central marketing tool, we are forced to face the harm that we can do to ourselves and to society and social relations through abuses that technology make possible. As information becomes more and more central, we will also realize the vulnerability of networks. Unfortunately, sabotaging a corporate or national information network is easier than sabotaging the industrial network; the links are more fragile, and the interdependence greater. The need for safeguards against industrial and national information espionage and sabotage are great and pressing.

To mention or raise these issues is not to solve them. But we can develop the analyses and begin better to understand the nature of the Information Age and its promises and pitfalls for individuals and for society. This is the beginning of an ethical analysis of the Information Age.

Thesis V. Confronting the Communication Complex: Information without communication is useless, and communication without information is empty. The ethics of communication shares the podium with the ethics of information in the new Information Age.

Information is not useful, even if truthful and accurate, unless it is used. Hence it needs to be communicated. The communication process, which is developing at an exponential rate, is central to the Information Age. The virtues of truthfulness and accuracy carry over into communication. But there are elements of communication that pose their own ethical issues: communication of what, to whom, in what form?

In the Information Age the communication explosion has resulted in information overload. There is more information than any individual can absorb. The instantaneous communication made possible by computers and the Internet open the lines of communication to all, in an environment in which anyone can say or publish anything. There is no peer review or editorial overview before something gets published on the Web; and anonymity makes possible irresponsibility. In

the name of the freedom of speech that we so cherish, more and more is posted on the worldwide web under the guise of information. The result is that it is difficult to know what to believe and what to trust as reliable. The function previously filled by peer review, editors, and the cost of publication has been eradicated in Web publishing. We need some comparable authenticators, which I shall call authentication centers. In the industrial world Consumer Reports and similar independent groups could test and give impartial judgments about products. Similar independent authenticators are needed with respect to information on the Web. Which Web sites, for instance, which carry medical information are reliable and authoritative, and which are not? The need for centers of this type in all areas of information is crucial if people are to benefit from the information available, and if they are to be kept from being harmed by the available misinformation and falsehoods, whether deliberate or unintended.

The same is true with respect to business, both as consumers and as suppliers of information. The lines between information and advertising, between information and brain washing or manipulation, between information and self interest are crucial. Two instances illustrate the point.

One is the reviews of books that one sees if one goes to Amazon.com to buy books. The only way such reviews will carry weight with viewers is if they can be sure that the reviews are not simply paid for by the book publisher and that Amazon.com is not paid to promote the book. If either is the case, then the review should be identified as an advertisement, as advertisements are identified in newspapers. The function of authenticator and of advertiser must be kept separate.

The second is search engines that bring up as their first few entries in any search Web sites that pay to have their sites mentioned first. If search engines are to be trusted, then they should give the Web sites closest to what one requests in a search, not the site that pays the most. If the latter is the standard, then that should be clearly stated, lest once again the function between authenticator and advertiser become blurred.

In this brief discussion I have mentioned a number of other virtues besides truthfulness and accuracy--namely trust or trustworthiness, and reliability. The four go together and form the basis for a smooth functioning information processing system. The application of these four key virtues to business is part of the task for the business ethicist.

Thesis VI. The American Information Privacy Schizophrenia: The U.S. is schizophrenic about information privacy, wanting it in theory and giving it away in practice.

Information must be communicated, but it must itself also be about something. Information about people has become much more important than it was previously because of the great opportunity for a revolution in marketing in which manufacturers can target potential customers in ways not previously possible.

A commonly heard issue that arises in the Information Age is the question of privacy--a question about which there is great confusion and about which Americans in particular may be said to be schizophrenic. The privacy that many complain is being eroded is not being taken from us. Most of us are giving it away. This privacy, which I shall call personal information privacy, is

information about ourselves. Although some individuals and some privacy and other groups, such as the Computer Professionals for Social Responsibility, argue in favor of legislation protecting personal information privacy and claim that everyone has a right to such privacy, it is difficult to defend any strong sense of a right to such privacy when so many people blithely give the information away. Sometimes they do so for no return, sometimes for minimal return--such as the possibility of getting notification of products they may be interested in purchasing, and sometimes for more substantial gain.

The importance of personal information to business, and one American response to privacy, is illustrated by the extraordinary offer made by the small company Free-PC.com, which in February offered 10,000 (eventually to go to a million) Compaq personal computers free to those willing to provide a variety of different kinds of information about themselves (including their ages, interests, income and hobbies), to receive ads on the Internet, and to have their Internet activities tracked. That information is obviously worth more to the company than the price of a 333MHz computer with a 4 GB hard drive. The computer is free: it is the information about the users that is valuable. Whether giving up a large area of personal privacy is worth a computer might be a matter of debate and of personal choice. But it is difficult to defend any strong right to personal information privacy when so many value it so cheaply.

Rather than a right to personal information privacy, what most people seem to want is protection from harm as a result of the misuse of personal information about them. They fear identity theft, or credit card theft, or some harm--psychological or financial or physical--as a result of information about them being widely and easily available. It is not their privacy that is violated, but their sense of security. Yet the two issues are often confused and the arguments are similarly confused.

The Information Age is changing the nature of privacy. Nonetheless, as a society we have had almost no debate about what the legitimate limits on privacy are, why they are important, or what violates those limits. Since business is one of the two potential abusers of information--the other being government--this is a clear issue for business ethics. But it is one that has generated very little attention in the literature, and one about which most businesses still do not include anything in their codes.

Thesis VII. Mickey Mouse isn't a program: Information is very different from machines and tangible products, and so requires a new conception of property and property protection applicable to it.

Until fairly recently a copyright granted protection to the expression of ideas in books and similar forms for 28 years, renewable for another 28. The protected period was then changed to the life of the author plus fifty years and to 75 years for a corporate author. In 1998 Congress extended the already extended period to the life of the author plus seventy years and to 95 years for a corporate author. The change came just in time to save Mickey Mouse from falling into the public domain, much to the pleasure of the Walt Disney Company. On the other hand, when faced with the Y2K problem many computer software companies claimed that their products did not have to be year 2000 compliant until 1996, and some even argued until 1998, because the life of a program was at best two or four years before it became obsolete. Nonetheless, computer

programs are covered by copyright for the same 95 years that Mickey Mouse or the latest novel is covered. Does 95 years of protection make sense when the industry claims its products are obsolete after four years or less?

We can share information without depriving ourselves of its full use. It can be stolen from us without depriving us of its use. It is intellectual property. But just as we have not adequately discussed the changing nature of privacy, we as a society have not adequately discussed the changing nature of property applicable in the Information Age. We have sought to use traditional laws about copyright and patents, and have in the process caused a great deal of confusion. Instead of rethinking intellectual property in the Information Age, we have tried to make do with concepts and legal doctrines that were not constructed with thought of the kind of intellectual property that is emerging and that does not fit the old mold. What is fair and what is not are issues that form an important part of business ethics for the Information Age, and are issues that too few in the field presently address.

Conclusion

The upshot is that business ethicists have a whole range of issues to which they have scarcely turned their attention. Cartoonists make fun of the lack of computer literacy and savvy among the older generation and indirectly praise the ease and expertise with which the younger generation takes to the technology of the Information Age. They often hit the nail on the head. My hope is that you who are presently students and who grew up with computers and with information technology will carry out the marriage of business ethics and information technology that we so urgently need in the emerging Information Age.

Questions

Do you make the distinction between information ethics and data ethics?

My answer is no, because data, I take it, is simply what is entered into the computer. And data can be true or false, data can represent anything. Data may be useful, or may not be. So it's not clear what "data ethics" could be. Rather we can to talk about useful data, and useful data turns out to be true, which turns out to be information. Therefore, I think, we can talk about useful data from an ethical point of view. Data by themselves, since they can be right or wrong, representative or misrepresentative, appropriate or inappropriate, or anything else you like, are just what you enter. If you have garbage in, you get garbage out. Thus we can't talk meaningfully about "data ethics," whereas with respect to information, I tried to give you the virtues that are embedded in it and that are presupposed by it, and the problems that arise from it. I think we can do something with developing an ethics there, whereas with data as such, it is not clear what to do.

There's a lot of data that was collected traditionally by telephone companies that was considered very personal data, like, when you made a phone call, what number you made the phone call from, how long the phone call lasted and so forth. And it was very, very protected by the Baby Bells. As the digital services have come along, I understand more and more of that information is up for sale. And I was just wondering how Bell Atlantic

reconciles your philosophy, which kind of flies in the face of much of what I hear telephone companies are doing right now, with these new practices.

I think that's a valid question. Not only telephone services, but also a great many companies of all sorts are collecting information, or collecting data, if you like. Most of it, at least, is supposed to be information, that is, correct data about personal use and so on. And I've suggested what happens with data collected on the Internet. Is that okay or not, from an ethical point of view? That's the question. My answer is that I can't give a hard yes or no because I have to qualify whatever I say. I would prefer to know how the information is being used, who's collecting it, what they're collecting, and what they're doing with it. And if I know that, then I would be able to say whether I approve or disapprove, whether it's okay with me that they do that or not with information about me. What bothers me is that all this information about me is being collected without my knowledge and is being used in ways that I can only imagine, some of which may be harmful to me. Now, if I have a right to anything, it's a right to protect myself from harm. Consequently, I have to ask how can I implement that right? And the only way I can implement that is to know that I may be harmed, and to know that I have to know what people are doing that may be linked to the harm that I might suffer. So, I would like to see companies very much up front telling us: "When you do this, that or the other thing, we're collecting information about you. We're collecting information on use and we're going to sell that information, we hope, in ways that you will approve of, to bring you products that we hope will interest you. But, if you're not interested in that, then let us know and we won't do it for you anymore. We'll take you off our list, we won't track you the way we track other people, and so on." Some companies do this. Or, a company might say, "We collect information about you of this type, but it will just be for our own personal use, that is, company use, not for use by other corporations, and we won't sell it or give it to others without your permission." Legislation in Europe has gone in the latter direction. There's presently legislation that has been passed in countries of the Europe Union that says that if one company collects this sort of information, it's not allowed to sell it to another company. America has not come to the point where we're willing to even entertain that legislation. And if it was proposed in Congress, I doubt whether it would pass, because the business interests against it are so strong. Now, what's the popular opinion on the issue? Well, I said, we're schizophrenic. There is no popular opinion. If I take one poll of this set of people and another of another set of people, I'm going to get different results. So, I think we have to decide what's really in our interest, and the only way we can decide that is by discussing the issue openly. Consequently, I'd like questions like yours to appear in periodicals, in the newspaper, in business ethics centers, in all sorts of places, so that we can talk about these things rationally rather than just letting them happen.

I view the development of the computer akin to the Thompson submachine gun which went through a period where it was appropriate during World War I, not appropriate for use by Prohibition periods, it's now banned as an assault weapon, and so forth. I take it you're uncomfortable with allowing technology to find its own level. In other words, you appear to feel that there should be some government or some societal regulation along the way. I'll have to tell you, I'm particularly troubled about the freedom of speech aspect. I'm sort of a Samuel Gompers person who doesn't just have to say things that are accepted and viewed and common but who can say what's new and different even though it does a harm. I'm

troubled with the idea that information which is so important and precious, faces the possibility of being controlled and not allowed to find its own level.

You asked two questions. Let me give you two answers. First, with respect to the information issue, my claim was not that we should prevent quacks from putting out their medical remedies on the Web, but that we should have authentication pages which will say, "If you're interested in cures for cancer, we have investigated and can report that these sites give information that is in accordance with the best known medical advances of the day." The quack sites can still operate - freedom of speech operates. Nobody says you can't have a quack site. Nobody outlaws them, nobody does anything to them. And, if you're interested in cures for cancer and you want to try those, you're free to do so. But, it would be nice to have someplace to go to say, "Hey, how do I, a poor novice, who's not a doctor, who doesn't know much about medicine, sort out what's reliable and what's not reliable out there?" Therefore, I proposed my authentication centers. I didn't intend them to be censorship centers and I didn't intend them to be run by the government.

My example with respect to products was Consumer Reports, which people can use or not use, which is independently funded, not sponsored by any corporation, which tries to be objective, and which a lot of people think serves a useful function. I'd like to have similar authentication centers developed in the various areas of information. So, I'm all with you about freedom of speech. I'm not in favor of outlawing that and I'm in favor of letting a hundred flowers bloom. Some of them will be useful and some of them will not.

On the other point, should we allow technology to go wherever it wants? Well, that's what I called the technological imperative, which says that technology has its own rationale and whatever is rational from its point of view will be developed by somebody and something will come out. And the question is one that Joseph Weizenbaum, a computer scientist from M.I.T., raised back in the seventies: Are there directions that we really shouldn't encourage? Maybe we can't outlaw developments, but are there directions in which we shouldn't encourage technology to go? Are there things that are obscene, that it would just be terrible to have technology develop? I think that's a legitimate question. Now, I haven't given you a definite answer. But I don't think the answer is: obviously no, we can't stop technological progress, anything anybody wants to develop is okay.

In the field of cloning, we've said, "Well, maybe we're not ready for human cloning yet," and some countries have imposed a moratorium on human cloning. Are there things in the technological realm that are similar to that which affect human beings very centrally and very directly and about which we'll want to say, "No, we don't think that should be done"? If so, we certainly shouldn't put government resources there, and we should discourage private resources from going in that direction. It would be nice to have a debate about the issue. I'd like to engage you in that debate and have you tell me why we shouldn't have any restrictions and then see if I could think up some things that I would think would be wrong to develop and see where we get. We now say we don't want to develop biological warfare agents. Those are bad things to develop and although we find countries developing them, we say that it's a no-no, we discourage such development, and so on. We don't want countries to proliferate nuclear bombs, because they pose a big threat to us all. Are there comparable things in the Information Age, such that would subvert the Information Age itself? If there are, then we should give very serious thought to

whether those should be developed and whether we should take precautions against their being developed and, if they are developed, precautions against their being used.

You talked about the issue of the Y2K problem and you said that it will cost about $ 600 billion dollars to fix the problem. My question is: The inventors of computers or software, didn't they predict what would happen? Well, what was, in both cases, the ethical approach you think they used if they predicted or if they did not predict the Y2K problems since it concerns us?

I wrote an article on that so I can refer you to the article ["Computers, Ethics and Business," Philosophic Exchange, (28), 1997-98, pp. 45-55]. The brief answer is, I think, that many of the computer scientists were aware that there was the problem. Some of them tried to bring it to the attention of management. The first time that I know of that it came up was in the 1970s, when we had the first warning, and this was from someone at IBM. It was acknowledged that it was a problem, but it was expensive to fix and it was twenty or more years off. It's hard to get a manager to make a change twenty years in advance of the real problem and, consequently, there was delay after delay after delay. If you try to ask who was ethically responsible at what point, you have to track through the particular developments and see. I think it's a worthwhile process and when I tried to do it, I thought that it was the responsibility of the programmers to inform management and those who didn't inform them in a timely fashion of the problem, I think, were ethically at fault. Then, I think, the onus shifted to management to make an appropriate decision. Managers had to weigh a great many different things and we can't say that every manager who delayed making the change acted unethically. It depends how much more the delay would cost. If they did not make the correction simply because it was too expensive, because they knew that they wouldn't be held responsible for not making the change, and because they would let somebody else take the blame when everything hits the fan, they were at fault. We can develop and describe a lot of different scenarios, so it's hard to say everybody's to blame. But, I think specific people are to blame at specific points, ethically, although I've never seen an article except my own that says anybody is ethically to blame for anything in this area.

Finally, if you look at programmers and companies that were putting out new programs in 1997 that weren't Year 2000 compatible, their excuse was: "Oh, in two years they have to buy a new version." That sounds to me unethical, unconscionable. They say, "I'm selling you a product that I know has this big glitch in it. It won't work in two and a half years, but that's tough. I won't tell you this in advance and when Year 2000 comes, you'll have to come around and spend another 60 bucks to buy the new, improved version." I think those companies acted unethically.

The computer people have said 1996 is the year that we start saying programs and computers should have been compliant. Why 1996 instead of 1995? Or 1994? Or 1990? They knew the problem in all the earlier years. Why pick 1996? Well, the argument, maybe, is that a computer is obsolete after four years. I don't know how many of you have computers older than four years. A lot of people do. Or perhaps the claim of those who sell computer programs is that the program is obsolete after four years. I'm still using programs from more than four years ago. Of course, there are later versions. So, these are all issues to which I don't want to give you definitive, ethical answers. But I would like to raise the problem, and have people ask the question you ask, and have them continue to ask it, so that we dissolve the Myth of Amoral

Computing and Information Technology and get managers and computer people to acknowledge that there are ethical issues and that they should take ethical responsibility for what they do.

Mike Hoffman: I'm going to take the prerogative of asking the last question. I'm going to ask it in under 15 seconds and I only ask that you will try to give your answer in about 2 or 3 minutes because we're already at a deadline. The question has to do with corporations and other organizations who sometimes and sometimes not, let employees know that they can break in, and may break in, on their email and monitor it at any time, for any reason. I wonder if you could comment in our privacy schizophrenic mode that we're in at the moment, as to how you come down on that issue, or at least some thoughts of yours on that issue.

My basic approach to that is that I think what employees are ethically or morally deserving of is information about what the company is doing with respect to monitoring their email or their Web use and what use will be made of that information. If a company is routinely monitoring or randomly monitoring email use to see if people are using email for personal use instead of business use, and if it has promulgated very clearly a policy that says, "You will not use email for personal use; you can only use your computer at work for business use, and if we find that you're using it for personal use, we take a very dim view of that and you'll be penalized in some way or another," then, I think the employees know the rules and either decide that the company is worthwhile working for and that they can live with the policy; or they'll decide, "Hey, I don't like this company. I'll move elsewhere." Or they'll say, "Well, if they're going to take that view of email, I'll use the telephone or I'll use some other means and I won't be tracked and I won't be monitored." Those are different reactions. The company has to decide what it wants as its rules, promulgate them, and then worry about the results. The employee has to obey the rules and then, if they don't like the rules, either leave or get around them in some way. And, I think many of the various options can be said to be ethical. So I don't know any way that I can argue that any company that monitors employees' email, even though it informs them of that practice, is unethical. The results may be counterproductive, be bad for employee morale, or have other negative impacts, but I really can't say that that is an unethical policy. A policy of monitoring may be unwise or counterproductive, but that is another matter. Companies are within their legal rights to monitor employees' email, and I believe that they have the ethical right to do so if they clearly inform the employees of the company's policy.

Biography

Richard T. De George is the University Distinguished Professor of Philosophy and Business Administration and the director of the International Center for Ethics in Business at the University of Kansas. He has authored more than 150 articles and 18 books including Ethics, Free Enterprise, and Public Policy (Oxford, 1978); Business Ethics (5th ed., Prentice Hall 1999); and Competing With Integrity in International Business (Oxford 1993).

De George, who received his PhD from Yale University, has been a research fellow at Yale University, Columbia University, Stanford University and the Hoover Institution. He serves on the editorial boards of several business ethics journals, consults on business ethics for a number of firms, and provides executive training on ethics and humanities to a variety of businesses and academic groups.

In 1996, De George -- along with Nelson Mandela and Bill Gates -- received an honorary doctorate from the Netherlands Business School. He is president of the International Society of Business, Economics, and Ethics and previously served as president of the American Philosophical Association and the Society for Business Ethics.