The Ethics of Information Technology and Business

Richard T. De George

Blackwell
Publishing

The Ethics of Information Technology and Business

Foundations of Business Ethics

Series editors: W. Michael Hoffman and Robert E. Frederick

Written by an assembly of the most distinguished figures in business ethics, the Foundations of Business Ethics series aims to explain and assess the fundamental issues that motivate interest in each of the main subjects of contemporary research. In addition to a general introduction to business ethics, individual volumes cover key ethical issues in management, marketing, finance, accounting, and computing. The volumes, which are complementary yet complete in themselves, allow instructors maximum flexibility in the design and presentation of course materials without sacrificing either depth of coverage or the discipline-based focus of many business courses. The volumes can be used separately or in combination with anthologies and case studies, depending on the needs and interests of the instructors and students.

Series List:

1 John R. Boatright: *Ethics in Finance*
2 Ronald Duska and Brenda Shay Duska: *Accounting Ethics*
3 Richard T. De George: *The Ethics of Information Technology and Business*

The Ethics of Information Technology and Business

Richard T. De George

Blackwell
Publishing

350 Main Street, Malden, MA 02148-5018, USA
108 Cowley Road, Oxford OX4 1JF, UK
550 Swanston Street, Carlton South, Melbourne, Victoria 3053, Australia
Kurfürstendamm 57, 10707 Berlin, Germany

First published 2003 by Blackwell Publishing Ltd

Library of Congress Cataloging-in-Publication Data

De George, Richard T.
The ethics of information technology and business / Richard T. De George.
p. cm. — (Foundations of business ethics ; 3)
Includes bibliographical references and index.
ISBN 0-631-21424-0 (hardcover) — ISBN 0-631-21425-9 (pbk.)
1. Business ethics. 2. Information technology—Moral and ethical aspects. I. Title. II. Series.
HF5387.D383 2003
174′.4—dc21
2002005756

A catalogue record for this book is available from the British Library.

Typeset in 10.5/12.5 Plantin
by SetSystems Ltd, Saffron Walden, Essex
Printed in United Kingdom
by MPG Books, Bodmin, Cornwall

For further information on
Blackwell Publishing, visit our website:
http://www.blackwellpublishing.com

Contents

Preface

By the mid-1990s business ethics was firmly established and widely accepted. Many businesses, especially the large corporations, had adopted some sort of code or value statement outlining proper behavior, the commitment of the company to ethical practices, and often a statement of morally praiseworthy aspirations or ideals. Many also had an ethics and a social responsibility component in their employee training programs. The importance of business ethics was stated by public figures from President Clinton to Secretary General of the United Nations, Kofi Annan. Business schools routinely had courses in business ethics, articles appeared in a variety of journals, both specialized and general. Academic research in the area was recognized as legitimate and conferences on business ethics issues had become commonplace.

By this time the major issues of the area encompassed by business ethics had been unearthed, discussed, and analyzed. Many of those were issues concerning the treatment of employees and of customers, truth in advertising, product safety, environmental protection, emerging global issues (such as the role of business in global warming), and international issues (such as bribery and child labor). Business, however, is a moving target. And at the same time that what are now considered standard issues in business ethics were acknowledged and to some extent resolved, business was evolving from the Industrial Age into the Information Age, and the United States was moving from an economy based on production to a service and information-based economy.

Ethical issues in business have a way of emerging only slowly and of being recognized even more slowly. Of course, the basic ethical norms prohibiting murder, stealing, lying, and so on, always apply. But issues about the ethics of new practices typically come into focus only after the practice has been in place for some time and the harm that the practice causes slowly becomes clear. This has been happening as business has changed in the recent period.

Computers have come to play a larger and larger role in business. The Internet is widely used in business as well as in homes, and business interests loom large in its development. Other technological advances from global positioning technology to cell phones to ever newly developed electronic marvels have been subtly changing the way business is done. In the process the new scenarios create new ethical challenges, which, as in the past, have first to be uncovered and then discussed and analyzed in an attempt to limit the harm done or threatened by them. Sometimes simply uncovering an ethical issue is sufficient to resolve it, for it will not be practiced in the light of day and it survives only when covert. Some unethical practices can be policed by those in the industry itself; others require legislation or social policy.

For a number of years there has been a debate among some academics about whether there is a field called "computer ethics" comparable to the fields of business ethics and medical ethics. Whether or not there is such a field, many of the issues that arise from the use of computers and from information technology more generally, have a connection in one way or another with business. There is clearly a computer industry, involving not only the creation of hardware but also of software. Computers are widely used in business, and although we would not talk about "typewriter ethics" simply because typewriters were (and still are) used in business, the use of computers in business has been sufficiently wide ranging to spawn a host of problems with an ethical dimension.

This book focuses on the ethical issues raised in businesses by computers and information technology. It looks both at the ethical issues for those in the computer and information technology industries and at the ethical issues raised by the use of computers and information technology for businesses in other industries. Many of the issues are still emerging, are not clear, and are the focus of debate about whether they are ethical issues and how they should be handled. Often, as with a newly emerging social innovation, the ethical issues have been ignored or submerged, not consciously or deliberately, but simply because the focus has been on development. In fact the development has been so rapid that society as a whole has not had the time to digest its ethical implications.

This fact has made this book difficult to write. On the one hand new issues are constantly emerging, so that any book of this type is necessarily incomplete and to some extent behind the newest issues before it emerges in print. On the other hand, some issues that are pressing at a given time are quickly left behind and become unimportant as technology develops and the issue is no longer center stage. A clear instance of this is what is known as the Y2K problem, or the worry about what would happen at the change of the millennium, since most programs were written using only the last two digits in specifying a year, and assumed "19" preceded those digits. Businesses and governments were forced to spend billions of dollars worldwide correcting computer code and ensuring that their programs and that airplanes and elevators would work properly with the change of centuries. As it turned out, business and government did act in time and January 1, 2000, arrived with no major disruptions anywhere in the world. There are lessons to be learned from that experience, but the Y2K problem is no longer a problem in the sense that it was prior to that January 1.

In writing this book I have developed in various ways four major interrelated themes. The first is what I have called the "Myth of Amoral Computing and Information Technology." This refers to the widespread phenomenon that the ethical dimension of computer and information technology development and use have been largely ignored both by those in the industry and by the general public. The second is the danger posed by the "Lure of the Technological Imperative," or the tendency to pursue technological development to the extent possible with little thought to the social implications and repercussions of such development. The third is the "Danger of the Hidden Substructure," which is in part a result of the fact that so much computer and information technological development and use take place behind the public scene and are not transparent to users or those affected by it, thus precluding public debate about the ethical impact of such development and use. The fourth theme is the "Acceptance of Technological Inertia" or the widespread failure to appreciate the fact that although computers and information technology have developed in certain ways, from an ethical point of view these are not necessarily the best ways they could have developed. Where this is the case, they can and should be changed. Computers and information technology should help and serve people and society. Where they do not, they should not be passively accepted. The four themes are sometimes stated explicitly, sometimes lurk in the background, where the attentive reader will see them. They are themes that I hope others will agree with and develop further. For this book has often done no more than raise them for discussion, and there is a great deal more to be done. In this way I consider this book a beginning, rather than the last word on any of the topics with which it deals.

Readers of this book may sometimes be frustrated, as I have been, by citations and notes to websites that no longer exist or no longer contain the information they contained when I used them. This, unfortunately, is one of the problems with electronic sources that is yet to be faced, much less resolved. Yet much information, both current and older, is so readily accessible on the Web, and is so often only accessible there, that reliance on it has become standard.

My special thanks go to my wife, who has endured my complaints and frustrations as my computer crashed or problems that were central faded to be replaced by others which had to be researched anew. I have tried out some of my ideas on students in my class on Moral Issues in Computer Technology, and I have learned a great deal from them about their perception of the issues. To them and unnamed others who have listened to my papers and presentations on ethical issues in information technology go my thanks.

Richard T. De George

chapter one

Ethics and the Information Revolution

One second after midnight January 1, 2000, marked a banner moment encapsulating the promise and problems of the new millennium, the age of the information revolution. At that moment all the computers of the world either recorded the date as 2000, 1900, or as some default date. If the computer registered 1900 or some default date in any of its operations, depending on its function, the results would range from the humorous or trivial to the serious. Many people had avoided flying the night of December 31, 1999, in order not to be caught in case of a disaster. The Chinese government had ordered airline executives to be aloft at midnight to guarantee that the proper computer corrections had been made and to offset the fears of the general population. Despite many worries and predictions, planes did not fall from the sky and most electrical grids operated. Potential disasters were averted. Yet the beginning of the new millennium was inextricably linked in the minds of many throughout the world with the realization of their dependence on the computer, on computer-embedded chips, and on the new technology that had emerged and had already taken society captive.

The Y2K problem, as it was called, is in some ways a uniquely computer problem. It has significant implications for business and for society as a whole, and is symptomatic of the extent to which the information society has integrated computers into everyday life and the extent to which we depend on computers.[1] Most often everyday use takes place without the typical person realizing the extent of the dependence, the consequences of such dependence, and the degree to which human beings have abdicated responsibility for what they do or for what happens to them as a result of such abdication. The Y2K problem thus provides a microcosm of a variety of ethical issues both individual and collective or societal.

The Y2K problem arose because in the early days of computers computer memory was so limited and precious that programmers sought every way possible to conserve it. One obvious way was to represent the year by only the last two digits rather than all four. Those who considered the problem at all back in the early days of programming may have felt that the problem, if there was one, could be easily fixed by a small patch at a later time when more memory became available. The problem became more and more serious as different programmers wrote different instructions to handle dates in the programs they developed. In addition they used early programming languages, such as COBOL, which were later superseded. Newer versions of a program were not completely rewritten. Rather they were added to, and new programs incorporated old routines or whole programs. By the 1990s many programs used by large businesses (as well as by government) included millions of lines of code, written over many years. No one knew exactly what was contained in all the lines or how dates and commands relating to them had been incorporated. Therefore no simple patch or program could be used to fix the situation. Because of different programming instructions and languages, not all the bugs or incompatibilities in large programs could be foreseen. Solving the problem, it was estimated in 1996, would cost an estimated US$600 billion worldwide.[2] Although the actual figure turned out to be considerably less, government and business in the United States alone spent approximately $34 billion to correct the problem.

Who was responsible for the costs, worry, and aggravation coming from this seemingly simple error? Surely the year 2000 did not come upon us unannounced.

Shareholders might hold company managers responsible for not preventing the inordinate costs of fixing a foreseeable difficulty. Managers might in turn hold the firm or person from whom the company bought the computer responsible. A software company could attempt to switch the blame onto the individual programmers who many years ago first introduced the problem in order to save memory space. They are like terrorists who set bombs to go off some period of time after they have left the scene. But surely the early programmers did not maliciously decide to use two digits instead of four. At the time and given the constraints under which they worked, this was a justifiable solution – or so they might well claim.

What the Y2K problems demonstrate very clearly is the subtle and not so subtle ways in which computers influence our lives, our dependence upon them, and the complicated issues they can raise concerning responsibility and the liabilities and obligations of business.

▲ THE INFORMATION REVOLUTION ▲

The Industrial Age has given way to the Information Age. Business is in the midst of adjusting to the information revolution. As it does, it faces new challenges, many of which have an ethical dimension and ethical implications. Information technology has changed and will increasingly change the way business is done. A business office without a computer has become almost a contradiction in terms. The days of the manual or of the electric typewriter are over. Retyping a page for two inverted letters, or retyping many pages for a missed line on the first page is grossly inefficient compared with entering the correction on the computer and printing out the new page or pages. That simple increase in efficiency is nothing compared to the time and effort saved with database manipulation, spreadsheets, and the host of programs available to secretaries and office workers today. Whether computers have increased overall productivity commensurate with their cost is still debated. But they have certainly increased efficiency in many areas.

The information revolution is not just one thing but it encompasses a great many different innovations. Essential to all of them is some aspect of what is generally termed "information," which is often used in a very broad and not very precise way. The information revolution includes, for instance, what is sometimes called the knowledge revolution.

The knowledge revolution refers to the exponential growth in knowledge in the past several decades. Our knowledge in the sciences is increasing at a rate far greater than at any time in the past. It increases so fast that no one can keep up with all the changes in any field, much less in all fields. The result is increasing specialization. Not only is the store of knowledge increasing, but it is increasingly being put to practical use. Inventions proliferate, as do startup companies anxious to bring them to market.

This is one aspect of knowledge. But knowledge is used in many ways, and businesses have found that although knowledge is power, knowledge is only productive if it is used. There is a tension in business between managers and senior executives wishing to keep much knowledge of the company and of its operations and functioning to themselves as a source of power and the need to share it and make it available to more and more employees so they can perform their functions better.

A third aspect of knowledge is the increase in knowledge that even entry-level members of the workforce need to perform their jobs. More education and training are needed not only to work on the new computers and manage the new programs, but also to learn how to learn in order to keep up with the rapid pace of change. If once a high-school education was sufficient for most jobs, that is no longer the case. The jobs requiring little or no knowledge have more and more been outsourced to developing countries where the cost of labor is comparatively cheap. This in turn raises problems about developing countries and possible exploitation.

What we refer to as knowledge is generally true or correct statements about the world. We sometimes use the term "information" in a similar way. Information is less global than knowledge, and is often discrete and disjointed. Bits of information go to make up the larger picture that we consider knowledge. Information may be trivial or important, useful or useless. Information overload consists in such a large amount of information that the user is unable to sort out the useful from the useless, the trivial from the important simply because of the sheer volume. Information overload is obvious to anyone who has sought information on the Internet and received several thousand hits when searching for a particular bit of information. Researchers encounter a similar problem when looking for information on a topic and being presented with thousands of articles and books somehow related to the topic with no indication of which are the best sources for which purposes. Information, like knowledge, is usually presumed to be true, although people do speak of false information and false knowledge, when it would be more accurate to speak of false beliefs.

"Data" is another term that is often used interchangeably with information. But while information usually refers to facts, or statements about the way the world is, data do not necessarily refer to facts. Data may represent information but they may also represent misinformation, they may be inaccurate, unreliable, and false. A problem with data is that, although they may be false or meaningless, once entered into computers they operate as if they represent information and are treated as if they do.

Information and data raise problems of their own for business and for those affected by business. Since the data often represent information about individuals, they are most useful if true. If inaccurate or false, they can affect individuals adversely, for instance, with respect to their credit ratings.

THE MYTH OF AMORAL COMPUTING AND INFORMATION TECHNOLOGY

The ubiquitousness of computers, highlighted by the Y2K problem, is one indication of the fact that developed societies have moved into a post-industrial age, frequently called the Information Age. Although this is widely acknowledged and often repeated, exactly what that means is vague. In part it means that what American society does primarily is not engage in the manufacture of products, even though it still does this, but that it engages in the generation, manipulation, and transfer of information. More people are engaged in this process than in the making of goods. Advances depend on knowledge and its application. The new breakthroughs are in computer technology, in biotechnology, and in information systems. Knowledge is readily at hand through the resources of the Internet. Anyone who wishes can develop a Web page. Computers can process information at incredible speeds and problems that took months to do by hand or calculator can now be done in minutes. We can test new designs by computer without having to actually build them; through techniques of virtual reality we can design and furnish our homes and walk through them before we begin construction. We can communicate with people anywhere in the world almost instantaneously through e-mail and the Internet. Governments are no longer able to block news of what happens in their countries through iron or bamboo or any other kind of curtain.

All of these changes have occurred with remarkable speed. They have in fact occurred with such speed that society has not had time to fully adjust to the changes, to experience and weigh the consequences, to pick and choose what is and what is not worth developing and what should be aborted before it develops further. Technology has developed faster than our evaluation of it, and the values society developed over centuries to cope with life in an agricultural and then in an industrial era are still the values that society holds and by which it lives. Businesses have sprung up to develop and exploit whatever is technologically possible before society has determined the overall social impact of such developments. The result has been the development of what I shall call the Myth of Amoral Computing and Information Technology, or MACIT.

The myth, like all myths, partially reveals and partially hides reality. We are all familiar with the excuse, made so often to customers by business representatives, "It's the computer's fault" or "computer error," as if the computer, and not some human being, were at fault or had made an error. The phrases are ways in which people and businesses say that they are not responsible for whatever it is that has happened and adversely affected someone else. The myth is expressed in language in which computers are the culprits, and of course, since computers are not moral beings, they can bear no moral responsibility. 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.

The truth is that often the operator or person at the terminal is not at fault and is struggling with something over which they have no control. What is covered up is the fact that somewhere in the process some human being is at fault or made an error. The implication that is often drawn is that since the mistake is the computer's, and the computer is not a moral being, there is no moral blame to be assigned, and no one to be held responsible or accountable. While it is true that the computer is not a moral being, it is not true that no one is or should be held morally responsible and accountable.

The Myth of Amoral Computing and Information Technology takes many forms. It does not hold that computing is immoral. Rather in holding that it is amoral MACIT says that it is improper, a conceptual mistake, to apply moral language and terms to computers and what they do. This much is correct. But what is false is that it is improper or a conceptual mistake to apply moral language and terms to what human beings do with computers, how they design, develop and apply them, how they manipulate and use information. Companies and schools order computers for all their employees or students, and anyone who is not computer literate will be left behind in the Information Age. This is not questioned, but is taken for granted. There is no debate about whether the members of society wish such a society and no discussion of how to guide the development of the society along these lines. What technology can do and can be developed will be done and developed. The MACIT implicitly sanctions this. According to the myth, these are not issues that have moral import or deserve moral scrutiny. Reality and progress march on, and attempting to stand in the way, slow the march, or evaluate them critically is to misconstrue the future. The result is resigned acceptance of what is developed and how.

The development of the Internet is a case in point. It has grown exponentially over a very short period of time. It crosses geographical borders with ease. It has many centers, its electronic packets pass over many different routes on their way from A to B. There is little regulation. It is perhaps the first instance of functional anarchy on a large scale. Its development has far outstripped societal debate about whether such a phenomenon is good or bad for all societies, and attempts at partial control by individual governments have quickly taught us that individual governmental control is at best difficult and often ineffective. The information revolution is descending upon societies that have not gone through the industrial revolution. And the MACIT accompanies each incursion into different societies.

The fact that the MACIT is a myth is not appreciated, not only by many ordinary people and most businesses, but also by many computer professionals, who see their task as technical, as pushing technology forward, as increasing speed and memory and computing capability, applying it wherever those who want it indicate and finding uses and applications others have not previously entertained. Computer professionals and computer-related businesses are often driven by fierce competition to get the next innovation first, to develop the new product or program before someone else does. For the pervading belief is that if it is possible someone will do it, and the first one to do it often captures the prize, whatever that is – riches, market share, fame. The result is that many do not take full responsibility for what they do or develop, they release products before they are adequately debugged and tested, and in other ways fail to consider the effects on people, which is at the heart of ethical thinking. The MACIT covers over their need to do so.

Another facet of the MACIT is that legislation has stepped in prior to ethical discussion, rather than as usual, following it. The typical pattern is for an action to be determined to be unethical or immoral, to harm people or society, and then to be legally controlled. But a result of the MACIT has been to preempt ethical discourse in this realm, and vested interests have prevailed in influencing legislation. The rules that we have and the laws that we have in this realm with respect to property and privacy, for instance, are most often not the result of widespread social discussion but are rather the result of lobbying, limited legislative hearings, and passage of bills dealing with issues that many of the legislators voting on them do not really understand.

Only slowly is the MACIT being uncovered and exposed for what it is – a partial story. Only slowly is society coming to grips with the changes that it is involved in. Only slowly are the members of society feeling the impacts of the information revolution sufficiently to begin attempting to evaluate it. A difficulty is that the revolution is a moving target, and even as society focuses on one part or issue, it tends to develop and evolve before closure is possible, and before all the facts can be properly evaluated, defensible conclusions drawn, and moral judgments rendered.

The reasons for the pervasiveness of the myth can be found to a large extent in the role of computer and information technology in society and to the nature of computers and information technology themselves. We can capture some of these in a variety of syndromes.

The ignorance syndrome

We have already noted how to most ordinary computer users, the computer is more or less a black box. They know how to use it and how to run various applications. But actual programming and fixing code is beyond their capabilities. To a large extent they are ignorant of the complexities and so rely on the experts. This in turn both helps relieve them of any feeling of responsibility when something goes wrong, and by extension, often leads to a feeling that things going wrong are normal and part of the price one pays for the new technology, and so not anything for which one holds others morally responsible.

The complexity syndrome

We have come to understand and accept that some programs are incompatible with other programs. Hence when something goes wrong, the ordinary computer user may not know whom to hold at fault or where to attribute blame. No one is responsible for making sure that operating systems and applications and a wide variety of applications are all compatible. If something goes wrong it is not unusual for each component maker to deny responsibility and to place the cause of the failure on some other component. The user has no way of knowing who is correct – or if there is any sense in which it is proper to ask who is correct.

The virtual reality syndrome

This is perhaps the most pervasive reason for the myth. What is done on the computer that interactively affects others – e.g., communicating by e-mail, entering another's computer, carrying on activities on the Internet – are all done in what is sometimes called cyberspace. There is no face-to-face meeting or confrontation, no physical trespass in the ordinary sense (since there is no real space involved). If one looks at a colleague's e-mail or computer files by entering his or her password, it is done from the privacy of one's room or office. This provides a psychic distance that seems to relieve one of responsibility or the feeling that one is really doing anything wrong. There is no physical harm done, to a large extent no tracks are left, no one is physically hurt. Ethics applies to the real world. Cyberspace is not the real world. And the notion of a cyber ethics appropriate to cyberspace has not yet become part of the general public's consciousness – nor of the consciousness of many in the computer and information technology field. That cyberspace is really part of the world in which we live and that what goes on there impacts real people and so is governed by the same ethical rules as all other areas of human activity is for the most part ignored or covered over.

This is the context in which business in the United States and in most of the industrially developed parts of the world finds itself. Business is an integral part of society and is neither in a privileged nor in an inferior position *vis-à-vis* the rest of society. Since the 1960s American business has been called upon more and more to hold itself morally or ethically accountable for what it does and for how it treats its workers, customers, suppliers, the environment, the communities in which it is located, and society at large. What can be called the Myth of Amoral Business, or the view that business is not appropriately held morally accountable for what it does, has largely been dispelled. But that part of it which overlaps with the MACIT remains.

THE MYTH OF AMORAL COMPUTING AND INFORMATION TECHNOLOGY AND THE Y2K PROBLEM

The Y2K problem provides an interesting mirror on the Myth of Amoral Computing and Information Technology. Although fixing the problem cost over $34 billion in the United States, there was no public discussion of moral responsibility, much less of any moral accountability or blame. Any moral judgment seems to have been irrelevant, and so, apparently, no one was to blame and no one was to be held accountable. The problem just "happened," like a force of nature which causes harm but for which no person is responsible.

One aspect of the application of the myth was to call the problem the "Y2K bug." A "bug" in a computer program is usually some defect in the program that is unknown to those writing the program and that appears only in use. Calling "Y2K" a bug, therefore, implies that programmers did not know that the year 2000 was coming and that assuming "19" before a date field of the remaining two places would cause problems starting with the year 2000. Of course they knew this. As we have seen most of the early computer programmers made a conscious decision to use only two places in order to save expensive memory – which they succeeded in doing.

Those who made and printed paper forms did not consider this a problem and reasonably assumed that people could properly interpret "'99" as the year 1999 and "'00" as the year 2000. It is likely, because it was so general a practice, that early programmers, who were interested in saving space, did not think of possible problems the convention might cause some thirty years later.

This is an explanation of why the convention in writing computer code developed and was followed. It says in effect that programmers were just like other people in using the convention and that they did not consider consequences thirty or more years away. Nor could they foresee the exponential growth of computer use. They in all likelihood did not imagine that the programs they wrote would be used and built on indefinitely and that they were writing in a sense for centuries.

There is no one we can point to who made the decision for a two-place year field, no one we can identify who started the convention. It is difficult morally to fault any individual in those days for not seeing ahead. Yet we can legitimately raise the question: should computer programmers have seen ahead? If the answer is no, then are we faced with a situation in which technology simply develops with no one being responsible for being conscious or aware of its implications, with no one taking responsibility for it, and with no one being accountable for how it develops and for the harm that it does? If so, this is a greater problem than the Y2K problem.

Somewhere along the line, as programmers built on previous programs and as they incorporated subroutines from other programs into their own, they must have realized that they were no longer sure of what a particular program contained or did not contain. It functioned as desired, but it was no longer the product of someone or some group that had mastery of the whole. Early programmers typically documented their programs. But documentation was often lost or ignored.

By the time some programmer or some manager discovered that they were no longer sure what their programs contained or how they were structured, the problem was that there might have been millions of lines of a program, and the cost of redoing it all from scratch would be enormous. At which point we begin to hold people responsible for what is in their programs and for what they sell or use is not entirely clear.

Moral responsibility requires causal responsibility or connection with the events in question, knowledge of what one is doing, and consent to doing it. Moral responsibility can be mitigated or lessened if any of the three conditions are not satisfied. The conditions which mitigate responsibility are known as excusing conditions, and they may excuse one from responsibility to a greater or lesser extent.

Surely all programmers in the 1950s, 1960s, and 1970s knew that the year 2000 was coming and that assuming the first two digits of the date as "19" would be valid only up through the year 1999. Bob Bemer, who worked for IBM, foresaw the problem in the 1970s, and suggested that the year field be four digits rather than two.[3] Obviously he was ignored.

Early programmers cannot claim ignorance of the fact that the year 2000 was coming as an excusing condition. Nor does the fact that people customarily wrote dates using the last two digits of the year provide an excuse. Yet I have suggested that because of the expense of computer memory in those decades, and the fact that the early programmers could not foresee the development of cheap memory or the fact that their programs would be built upon instead of being replaced, might provide some excuse and so some – or perhaps even complete – mitigation of moral blame.

If programmers in those decades could not foresee problems with the year 2000, programmers in the early 1990s were certainly close enough to consider what would happen with the close of the old century. Clearly someone at some point not only recognized the problem but started to do something about it. Those closest to the problem had the responsibility to foresee difficulties and to report that something had to be done. Since any firm that had been in business for more than a decade and used mainframe computers had the problem, all the companies should have been informed of it. It was then the responsibility of those with the authority to do something about the problem to take the appropriate action.

The likely scenario suggested by the Myth of Amoral Computing and Information Technology is that the general managers, who were not computer programmers and may have been barely computer literate, probably did not appreciate the enormity of the 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. In some instances managers saw that this was a problem that could be passed on to their successors, and that they would not be held responsible for not having acted in a timely fashion. They could avoid taking the financial hit during their tenure, leaving their replacement to come up with the needed money and to suffer any negative repercussions. The tendency to avoid taking responsibility for timely action seems to have been rampant.

Information Systems (IS) and Information Technology (IT) offices are not typically center stage at corporate headquarters, and the typical manager is not a computer techie. If presented early by their Information Systems people with the very large projected cost of correcting it, the general managers perhaps understandably did not immediately authorize the expenditure of millions of dollars for what seemed at the time a far off problem. Most firms had what plausibly appeared at the time as more immediate problems with which to deal. Understanding this reaction, however, is not the same as exonerating from moral responsibility those who had it, or for their delaying fixing it sooner rather than later, and thus at lesser rather than greater expense to the firm.

The delayed response to the Y2K problem indicates that management for the most part still tends to think of Information Systems and Information Technology as something that remains a service function of the corporation, off in a back set of rooms, instead of being prominently in the center of the corporation. The disconnection between corporate leaders and their technical divisions is the clearest indication that firms have not moved consciously into the Information Age. They are backing into it or being pulled by a technology they do not completely understand, even as they become more and more dependent on it. 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 it and take responsibility for it.

It is generally accepted that those who produce harm are responsible for the harm they cause. Corporations that harm their customers are morally and usually legally responsible for making good on the harm caused. We can trace the causal link back, as lawyers are wont to do. In the case of the user of a product that contains a program that causes the product not to operate as normally expected, the customer has recourse to the supplier of the product. If the product contained a program that is defective in some way, the producer may be the developer of the product or may simply have purchased or licensed the product or had it developed by a subcontractor. Responsibility for the program devolves then on the producer of the program. Programmers who work for an employer are responsible to the employer, but the employer owns their products as "work for hire" and so is responsible for the use to which it is put. Ethically each company bears responsibility for its products and for the harm it does by failures due to its products.

We can generalize beyond the Y2K problem. Those who produce or incorporate programs into products are responsible for those products and programs, just as they are responsible for other products or goods they sell. Yet there is a tendency which we have noted in the Myth of Amoral Computing and Information Technology for companies to disown responsibility for computer malfunctions or breakdowns, and for commercial software producers to issue disclaimers with their products claiming that by opening the product the user relieves them of all responsibility. That this has been accepted without much complaint by the general public is at best puzzling. One result has been for software producers to release their products before they are ready. Savvy software users know better than to purchase the first version of any new software product. Users have learned that instead of the extensive testing that should be done before a product is released, producers release a product which they know still has defects, and which they correct as the defects are reported to them. The general public thus provides some of the testing the producer should have done. Yet the buyer is not informed of this service to the producer, or paid for it if he or she reports a difficulty; nor does the product cost less because it has not been completely debugged when marketed. All of this is contrary to the general policy with respect to other products.

What has happened in these cases as with most other ethical issues related to computers is that the ethical dimension has been preempted by the legal dimension, and the laws have tended to reflect the business interests of the providers of computer programs and services.

Even in the 1990s, instead of changing all the old two-digit fields to four digits, many companies and programmers decided to stick with a two-digit field and rely on some fix such as to treat "00" as greater than "99" in fields dealing with years, or treating all dates lower than some number, e.g., "20" as being in the twenty-first century instead of the twentieth, a solution that will be good only until the year 2020 approaches. For some companies this is ethically responsible. For others it is not, and those responsible are simply shifting the problem forward, when it will be harder to fix.

There was no excuse in the late 1990s for programmers writing new programs to use two digits rather than four for years in new programs; yet many did, using some algorithm or other to keep the two centuries straight and assuming that there will never be a need for more than two centuries and that their programs will not be in use by the time the algorithm no longer works because of the next century. A lesson to be learned from the Y2K problem is that no one presently knows how long programs that are being written today will be embedded in programs used many years into the future, and that programmers have the moral responsibility to avoid problems that can be avoided, even if the problems are foreseeable only for the distant future.

The Y2K problem points to a larger and potentially more significant problem. With the thirty to forty year experience we have with computers and computer programs thus far, the Y2K problem demonstrates the extent to which society, government, and businesses, as well as individual users, are losing control over the programs that we use and have come to rely upon.

The Y2K problem arose in many cases because of early programming, which was often idiosyncratic in labeling and documentation. There were few imposed and widely recognized standards, since the standards had yet to be developed. Most of the programming was done in COBOL, which was widely taught in colleges, but which has long since been replaced by more advanced programming languages. Hence to correct the Y2K problem, step one was to find people who knew COBOL and could go back and read the old lines of instruction. The number of people proficient in COBOL was comparatively small, and a large number of those who worked on the problems were people who had retired and had been lured out of retirement by the high pay people with such knowledge commanded.

It does not take much imagination to see what would happen if a similar problem arose twenty years from now. The number of people skilled in COBOL would by then have shrunk to a very small number. Eventually the language will be unknown by any but perhaps historians of computer languages. By continuing to rely on old programs instead of rewriting them, as many companies did in correcting their Y2K problems, society as a whole could run the risk of eventually using and relying on programs that no one can fix, and that no one can even examine knowledgeably. Computers will be black boxes with output that one takes on faith without any experts to guarantee that what goes on within them is reliable. Nor is the problem only with COBOL. The life-span of computer languages is already incredibly brief. As programmers continuously incorporate older programming code into new programs or as they build on existing programs, it is not hard to foresee that society in general as well as governments, individual firms, and organizations will be relying on embedded code that no one can any longer read.

Because programs now often involve millions of lines of code, it is not possible for any single individual to write or rewrite it all. Nor would that be of particular use, since that person would then be the only one with command of the whole.

With loss of control there is a tendency to disclaim responsibility. If unforeseen and untoward events occur, they are blamed on the computer, which is to say that no blame is assigned or assumed.

Unforeseen computer events become unforeseeable computer events, which take on the status of acts of God. Only in this case God is the computer. Acts of God are events that typically are excluded from insurance policies, although one can insure against certain specific damages, such as that caused by flood or earthquake. Insurance companies might similarly start issuing computer damage insurance, or alternatively they might start excluding such harm from their umbrella or specific policies. This scenario accepts the current trend towards lack of control and lack of responsibility and accountability as inevitable. Such an attitude reinforces the cause and provides no incentive to find a way to reverse or push back or stop the loss of control. If no one is responsible for doing anything along these lines, no one will do anything to change present procedures or attitudes.

Since the new millennium arrived with no computer-related disaster, many adopted the attitude that Y2K had not been a problem after all, and that companies and governments and individuals had been subjected to some sort of scam or scare without foundation. In fact, however, it is only because those responsible did finally take corrective action at great cost that disaster was averted. The many law suits that had been feared did not materialize, and hence many felt that there was no need to look into the issue of responsibility or to worry about changing procedures that help people avoid accountability. The lack of disaster in turn reinforced the Myth of Amoral Computing and Information Technology. Yet the myth is not a solution but the heart of the problem, and Y2K illustrated its depth and pervasiveness.

INFORMATION, ETHICS, AND LAW

The Myth of Amoral Computing and Information Technology comes in many varieties. One is to equate whatever is required of anyone in computing or information systems with what is required by law. If it is legal, it is permissible. If it is illegal, it is not permissible. The view is a simple one, but it fails to capture the reality of the relation between law and ethics.

To begin with, the criminal law in general tends to make illegal what is unethical. In the obvious cases of murder, stealing, perjury, and the like, what is made criminal is what is unethical. The force of law is brought to reinforce the moral sanctions society already imposes for these actions. In the case of computer-related activities, part of the task before passing legislation is coming to a prior conclusion about the morality of new practices as they arise. Good legal practice allows people freedom of activity to the broadest extent possible compatible with a similar freedom for all. It does not criminalize activity unless it is harmful in some way, and so unless it is unethical. The decision of whether it is harmful and the extent thereof, and so whether it is unethical, is not decided by looking at law, but rather law looks at ethics. Because of this there is generally a lag of law behind ethics. Slavery was unethical before it was made illegal, as were discrimination and sexual harassment and other actions that in more recent times have been made illegal. We can and do consider actions or practices unethical before they are made illegal, and so should expect this to be the pattern with respect to computers and information technology. Spreading computer viruses that destroy the recipient's files or in other ways harm the recipient's files or computer was unethical before it was made illegal.

A second reason we should not equate law with ethics is that we can evaluate any law from an ethical point of view, asking, is it in fact a just or good law? Some laws, such as the apartheid laws in South Africa that enforced segregation and discrimination against black people in that country, are unethical. In such cases, they should be repealed. If law and ethics were identical, there would be no way to raise the issue of whether the law was ethically defensible, which is clearly not the case. Hence just because something is either permitted or prohibited by law with respect to computers does not necessitate the conclusion that it is a just law, although the presumption is generally in favor of that assumption.

Third, not everything that is unethical can or should be made illegal. Not everything that is unethical can be made illegal because the sphere of ethics is very broad and allows of degrees. Not every lie is illegal, even though lying in general is unethical. The law singles out certain categories with respect to truth telling, and, for instance, prohibits perjury, and false advertising, but not instances of one individual's lying to another on private matters. It would be impossible to police a law that prohibited all lying, and one result would be to inculcate disrespect for the law. This leads to the reasons why not all unethical activity, even if it could be made illegal, should be made illegal. The cost of enforcing the law might be more than the good obtained by having the law; the harm done by the unethical practice might be negligible; the practice might not be widespread enough to make illegal; the wording of the law might not be able to capture the wrong without also outlawing permissible behavior, and so on. The difficulty of drafting legislation that keeps pornography out of the view of children on the Internet while at the same time not violating the rights of adults to freedom of speech and of access to what they wish to view is an instance of this. Until proper language can be drafted, no legislation is appropriate. Yet the pandering of pornography to minors is arguably unethical.

Although the relation of ethics and law puts the priority on ethics before law, there is a relation in the other direction. Although some actions in themselves, such as murder, are morally wrong, most actions are morally neutral. Yet some of them become actions that we are to avoid simply because they are made illegal. Whether one drives on the right hand side of the road or on the left hand side is in itself a matter of moral indifference. Nonetheless, it is clear that if people are to get anywhere quickly and efficiently, there should be some agreement on which side of the road to drive on. Otherwise people will continually be in each other's way, and traffic will get nowhere. Since the side of the road on which people drive is in itself not an ethical matter, there is no ethically correct side on which to drive. But once a country decides that all traffic will drive on the left, for instance, then not to drive on the left is to endanger both oneself and others, as well as to undermine efficiency. Hence, once a country legislates that traffic is to move on the left, it becomes ethically required that one drive on the left. In this case it is ethically required not only because not to do so threatens harm but also because it is required by law. Once a law is passed, therefore, an action that was previously permitted may now be legally prohibited, and hence at least indirectly unethical. In general there is an ethical obligation to obey just laws. Just laws are laws that do not require that one do anything that is unethical, and that are in general passed in the appropriate way and passed for the common good. The presumption generally is that laws are to be obeyed. In a defensible legal system laws are passed for the common good, and to go against the common good by breaking the law is in general prima facie wrong. Thus, in a system of law that is generally ethically defensible, not only do laws carry with them legal obligations, but one also has the moral or ethical obligation to obey them. Civil disobedience, which consists in breaking a just law to protest an unjust one, might be justified, but the onus is on those who would break the law, and the permissible means for expressing civil disobedience have to be met.