SECOND EDITION

COMPUTER ETHICS

CAUTIONARY TALES AND ETHICAL DILEMMAS IN COMPUTING

TOM FORESTER AND PERRY MORRISON

Ethics
Cautionary Tales and Ethical Dilemmas in Computing

Second Edition

Tom Forester and Perry Morrison

The MIT Press
Cambridge, Massachusetts
London, England

Third printing, 1995

This book was set in Sabon by .eps Electronic Publishing Services and was printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Forester, Tom.
Computer ethics : cautionary tales and ethical dilemmas in computing / Tom Forester and Perry Morrison.—2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 0-262-06164-3 (hc).—ISBN 0-262-56073-9 (pbk.)
1. Electronic data processing—Moral and ethical aspects.
I. Morrison, Perry. II. Title.
QA76.9.M65F67 1994
174′.90904—dc20 93-22874
CIP

Also by Tom Forester

The Microelectronics Revolution (ed.) (1980)
The Information Technology Revolution (ed.) (1985)
High-Tech Society: The Story of the Information Technology Revolution (1987)
The Materials Revolution (ed.) (1988)
Computers in the Human Context (ed.) (1989)
Silicon Samurai: How Japan Conquered the World's IT Industry (1993)

Preface and Acknowledgments

The aim of this book is twofold: (1) to describe some of the new problems created for society by computers, and (2) to show how these problems present ethical dilemmas for computer professionals and computer users.

The problems created by computers, in turn, arise from two main sources: from hardware and software *malfunctions* and from *misuse* by human beings. We argue that computer systems have often proved to be insecure, unreliable, and unpredictable and that society has yet to come to terms with the consequences. We also seek to show how society has become newly vulnerable to human misuse of computers in the form of computer crime, software theft, hacking, the creation of viruses, invasions of privacy, and so on.

Computer Ethics has evolved from our previous writings and in particular our experiences teaching two courses on the human and social context of computing to computer science students at Griffith University in Australia. One lesson we quickly learned was that computing students cannot be assumed to possess any awareness of social trends, global problems, or organizational issues. Accordingly, these courses have been reshaped in order to relate more closely to students' career goals by focusing on the ethical dilemmas they will face in their everyday lives as computer professionals.

Many college and university computer science (CS) degree programs are now including or seeking to include an ethics component along the lines of the Social, Ethical and Professional Context (or SP) stream outlined in the recent ACM/IEEE-CS Curriculum Task Force report (reproduced in appendix B). Their plans in the past have been hampered by a lack of suitable teaching texts. *Computer Ethics* has been designed to help fill that gap and to fit squarely into the recommended CS curriculum as one of the nine key areas of a model CS degree. For this reason, we have included numerous up-to-date references as well as hypothetical scenarios and role-playing exercises at the end of the book. The creative teacher should be able to build on these and thus be in a position to deliver a lively and engaging course.

Readers will notice that we have avoided lengthy discussion of philosophical and ethical theory. The reason is that this book is but a first step, with the simple aim of sensitizing undergraduate computing students to ethical issues. It is, as one reviewer of the first edition put it, a "consciousness-raising" exercise, providing a "wake-up call" to students, computer users, and computer professionals. Thus we have placed emphasis on attention-grabbing cases and memorable anecdotes: much can be learned from such cautionary tales, which have been a traditional method of socializing newcomers into professions.

Nor will readers find a detailed account of the legislative positions around the world on the various issues discussed. In each country the legal situation is often complex, confused, and fast-changing—and again this is not the purpose of the book.

Finally, a note on sources. First, we have to acknowledge an enormous debt to Peter G. Neumann, whose "Risks to the Public in Computer Systems" sections in *Software Engineering Notes,* the journal of the Association of Computing Machinery's Special Interest Group on Software (ACM-SIGSOFT), have provided inspiration, amusement, and a vast amount of valuable information. Long may he continue. Second, we have to caution that many of these and other sources are newspaper and media reports, which, like computers, are not always one-hundred percent reliable.

Computer Ethics

Contents

1

Introduction: Social, Ethical, and Professional Issues in Computing

Computers are the core technology of our times. They are the new paradigm, the new "common sense." In the comparatively short space of forty years, computers have become central to the operations of industrial societies. Without computers and computer networks, much of manufacturing industry, commerce, transport and distribution, government, the military, health services, education, and research would simply grind to a halt.

Computers are certainly the most important technology to have come along this century, and the current Information Technology Revolution may in time equal or even exceed the Industrial Revolution in terms of social significance. We are still trying to understand the full implications of the computerization that has already taken place in key areas of society such as the workplace. Computers and computer-based information and communication systems will have an even greater impact on our way of life in the next millennium—now just a few years away.

Yet as society becomes more dependent on computers and computer networks, we also become more and more vulnerable to computer malfunctions (usually caused by unreliable software) and to computer misuse—that is, to the misuse of computers and computer networks by human beings. Malfunctioning computers and the misuse of computers have created a whole new range of social problems, such as computer crime, software theft, hacking, the creation of viruses, invasions of privacy, overreliance on intelligent machines, and workplace stress. In turn, each of these problems creates ethical dilemmas for computer professionals and users. Ethical theory and professional codes of ethics can help us resolve these ethical dilemmas to some extent, while computing educators have a special responsibility to try to ensure more ethical behavior among future generations of computer users.

Our Computerized Society

When computers hit the headlines, it usually results in bad publicity for them. When power supplies fail, phone systems go down, air traffic control systems seize up, or traffic lights go on the blink, there is nearly always a spokesperson ready to blame the problem on a luckless computer. When public utilities, credit-checking agencies, the police, tax departments, or motor vehicle license centers make hideous mistakes, they invariably blame it on computer error. When the bank or the airline cannot process our transaction, we're told that "the computer is down" or that "we're having problems with our computer." The poor old computer gets the blame on these and many other occasions, although frequently something else is at fault. Even when the problem is computer-related, the ultimate cause of failure is human error rather than machine error, because humans design the computers and write the software that tells computers what to do.

Computers have been associated with some major blunders in recent times. For instance, the infamous hole in the ozone layer remained undetected for seven years because of a program design error. No less than twenty-two US servicemen died in the early 1980s in five separate crashes of the U.S. Air Force's Blackhawk helicopter as a result of radio interference with its novel, computer-based fly-by-wire system. At least four people died in North America because of computer glitches in the Therac-25 cancer radiotherapy machine, while similar disasters have been reported recently in England and Spain. During the 1991 Gulf war, software failure in the Patriot missile defense system enabled an Iraqi Scud missile to penetrate the U.S. military barracks in Dhahran, killing twenty-eight people, while the notorious trouble with the Hubble space telescope in the same year was exacerbated by a programming error that shut down the onboard computer.[1]

In fact, computers have figured one way or another in almost every famous system failure, from Three Mile Island, Chernobyl, and the Challenger space shuttle disaster, to the Air New Zealand antarctic crash and the downing of the Korean Air Lines flight 007 over Sakhalin Island, not to mention the sinking of HMS Sheffield in the Falklands war and the shooting down of an Iranian airbus by the USS Vincennes over the Persian Gulf. A software bug lay behind the massive New York phone failure of January 1990, which shut down AT&T's phone network and New York's airports for nine hours, while a system design error helped shut down New York's phones for another four hours in September 1991 (key AT&T engineers were away at a seminar on how to cope with emergencies). A whole series of aerospace accidents such as the French, Indian, and Nepalese A320 Airbus disasters, the Bell V-22 Osprey and Northrop YF-23 crashes, and the downing of the Lauda Air Boeing 767 in Thailand has been attributed to unreliable software in computerized fly-by-wire systems. Undeterred, engineers are now developing sail-by-wire navigation systems for ships and drive-by-wire systems for our cars.[2]

Computers and computer networks are vulnerable to physical breaches such as fires, floods, earthquakes, and power cuts—including very short power spikes or voltage sags ("dirty power") that can be enough to knock out a sensitive system. A good example was the fire in the Setagaya telephone office in Tokyo in 1984 that instantly cut 3,000 data and 89,000 telephone lines and resulted in huge losses for Japanese businesses. Communication networks are also vulnerable to inadvertent human or animal intervention. For instance, increasingly popular fiber optic cables, containing thousands of phone circuits, have been devoured by hungry beavers in Missouri, foxes in outback Australia, and sharks and beam-trawling fishermen in the Pacific Ocean. In January 1991, a clumsy New Jersey repair crew sliced through a major optical fiber artery, shutting down New York's phones for a further six hours, while similar breaks have been reported from Chicago, Los Angeles, and Washington D.C. The Federal Aviation Administration recently recorded the shutdown of four major U.S. air traffic control centers. The cause? "Fiber cable cut by farmer burying dead cow," said the official report.[3]

Computers and communication systems are also vulnerable to physical attacks by humans and to software sabotage by outside hackers and inside employees. For example, a saboteur entered telecommunications tunnels in Sydney, Australia, one day in 1987 and carefully severed twenty-four cables, knocking out 35,000 telephone lines in forty Sydney suburbs and bringing down hundreds of computers, automated teller machines (ATMs), and point of sale (POS), telex, and fax terminals with it. Some businesses were put out of action for forty-eight hours as engineers battled to restore services. Had the saboteur not been working with an out-of-date plan, the whole of Australia's telecommunications system might have been blacked out. In Chicago in 1986, a disgruntled employee at Encyclopaedia Brittanica, angry at having been laid off, merely tapped into the encyclopedia's database and made a few alterations to the text being prepared for a new edition of the renowned work—like changing references to Jesus Christ to Allah and inserting the names of company executives in odd positions. As one executive commented, "In the computer age, this is exactly what we have nightmares about."[4]

Our growing dependency on computers has been highlighted further in recent years by such incidents as the theft in the former Soviet Union in 1990 of computer disks containing medical information on some 670,000 people exposed to radiation in the Chernobyl nuclear disaster. The disks were simply wiped and then resold by the teenaged thieves. In 1989, vital information about the infamous Alaskan oil spill was "inadvertently" destroyed at a stroke by an Exxon computer operator. In the same year, U.S. retailer Montgomery Ward allegedly discovered one of its warehouses in California that had been lost for three years because of an error in its master inventory program. Apparently, one day the trucks stopped arriving at the warehouse: nothing came in or went out. But the paychecks were issued on a different system, so for three whole years (so the story goes) the employees went to work every day, moved boxes around, and submitted timecards—without ever telling company headquarters. "It was a bit like a job with the government," said one worker after the blunder had been discovered.[5]

In Amsterdam, Holland, in 1991, the body of an old man who had died six months earlier was found in an apartment by a caretaker who had been concerned about a large pile of mail for him. The man had been something of a recluse, but because his rent, gas, and electricity bills were paid automatically by computer, he wasn't missed. His pension also had been transferred into his bank account every month, so all the relevant authorities assumed that he was still alive. Another particularly disturbing example of computer dependency came from London during the Gulf war, when computer disks containing the Allies' plans for Desert

Storm disappeared, along with a lap-top computer, from a parked car belonging to Wing Commander David Farquhar of the Royal Air Force Strike Command. Luckily for the Allies, the thieves did not recognize the value of the unencrypted data, which did not fall into Iraqi hands. But a court martial for negligence and breach of security awaited Farquhar.[6]

Computers are changing our way of life in all sorts of ways. At work, we may have our performance monitored by computer and our electronic mail read by the boss. It's no good trying to delete embarrassing e-mail statements because someone probably will have a backup copy of what you wrote. This is what happened to White House adviser Colonel Oliver North and to John Poindexter, the former national security adviser to president Ronald Reagan, when they tried to cover up evidence of the Iran-Contra scandal. Poindexter allegedly sat up all night deleting 5,012 e-mail messages, while North destroyed a further 736, but unknown to Poindexter and North the messages were all preserved on backup tapes that were subsequently read by congressional investigators. And if you use a spell-checker or language-corrector in your word processing program, be sure that it doesn't land you in trouble. For example, the Fresno Bee newspaper in California recently had to run a correction that read: "An item in Thursday's Nation Digest about the Massachusetts budget crisis made reference to new taxes that will help 'put Massachusetts back in the African-American.' This item should have read 'put Massachusetts back in the black.'"[7]

Recent government reports have confirmed that our growing dependence on computers leaves society increasingly vulnerable to software bugs, physical accidents, and attacks on critical systems. In 1989, a report to the U.S. Congress from one of its subcommittees, written by James H. Paul and Gregory C. Simon, found that the U.S. government was wasting millions of dollars a year on software that was overdue, inadequate, unsafe, and riddled with bugs. In 1990, the Canadian auditor-general, Ken Dye, warned that most of the Canadian government's computer systems were vulnerable to physical or logical attack: "That's like running a railroad without signals or a busy airport without traffic controls," he said. In 1991, a major report by the System Security Study Committee of the U.S. National Academy of Sciences, published as Computers at Risk, called for improved security, safety, and reliability in computer systems. The report declared that society was becoming more vulnerable to "poor system design, accidents that disable systems, and attacks on computer systems."[8]

Some New Social Problems Created by Computers

Although society as a whole derives benefit from the use of computers and computer networks, computerization has created some serious problems for society that were largely unforeseen.

In this book, we classify the new social problems created by computers into seven main categories: computer crime and the problem of computer security; software theft and the question of intellectual property rights; the new phenomena of hacking and the creation of viruses; computer unreliability and the key question of software quality; data storage and the invasion of privacy; the social implications of artificial intelligence and expert systems; and the many problems associated with workplace computerization.

These new problems have proved to be costly: computer crime costs companies millions of dollars a year, while software producers lose staggering sums as a result of widespread software theft. In recent years, huge amounts of time and money have had to be devoted to repairing the damage to systems caused by the activities of malicious hackers and virus creators. Unreliable hardware and software costs society untold billions every year in terms of downtime, cost overruns, and abandoned systems, while invasions of privacy and database mix-ups have resulted in expensive lawsuits and much individual stress. Sophisticated expert systems lie unused for fear of attracting lawsuits, and workplace stress caused by inappropriate computerization costs society millions in absenteeism, sickness benefits, and reduced productivity.

Computer crime is a growing problem for companies, according to recent reports. Every new technology introduced into society creates new opportunities for crime, and information technology is no exception. A new generation of high-tech criminals is busy stealing data, doctoring data, and threatening to destroy data for monetary gain. New types of fraud made possible by computers include ATM fraud, EFT (electronic funds transfer) fraud, EDI (electronic data interchange) fraud, mobile phone fraud, cable TV fraud, and telemarketing fraud. Desktop printing

(DTP) has even made desktop forgery possible. Perhaps the biggest new crime is phone fraud, which may be costing American companies as much as $2 billion a year. Most analysts think that reported computer crime is just the tip of an iceberg of underground digital deviance that sees criminals and the crime authorities competing to stay one jump ahead of each other.

Software theft or the illegal copying of software is a major problem that is costing software producers an estimated $12 billion dollars a year. Recent cases of software piracy highlight the prevalence of software copying and the worldwide threat posed by organized software pirates. Computer users and software developers tend to have very different ethical positions on the question of copying software, while the law in most countries is confusing and out of date. There is an ongoing debate about whether copyright law or patent law provides the most appropriate protection for software. Meanwhile the legal position in the United States, for example, has been confused further by the widely varying judgments handed down by U.S. courts in recent years. The recent rash of look and feel suits launched by companies such as Lotus and Apple have muddied the waters still further. The central question facing the information technology (IT) industry is how to reward innovation without stifling creativity, but there is no obvious answer to this conundrum and no consensus as to what constitutes ethical practice.

Attacks by hackers and virus creators on computer systems have proved enormously costly to computer operators. In recent cases, hackers have broken into university computers in order to alter exam results, downloaded software worth millions, disrupted the 911 emergency phone system in the United States, stolen credit card numbers, hacked into U.S. military computers and sold the stolen data to the KGB, and blackmailed London banks into employing them as security advisers. Hackers also have planted viruses that have caused computer users untold misery in recent years. Viruses have erased files, damaged disks, and completely shut down systems. For example, the famous Internet worm, let loose by Cornell student Robert Morris in 1988, badly damaged 6,000 systems across the United States. There is ongoing debate about whether hackers can sometimes function as guardians of our civil liberties, but in most countries the response to the hacking craze has been new security measures, new laws such as Britain's Computer Misuse Act