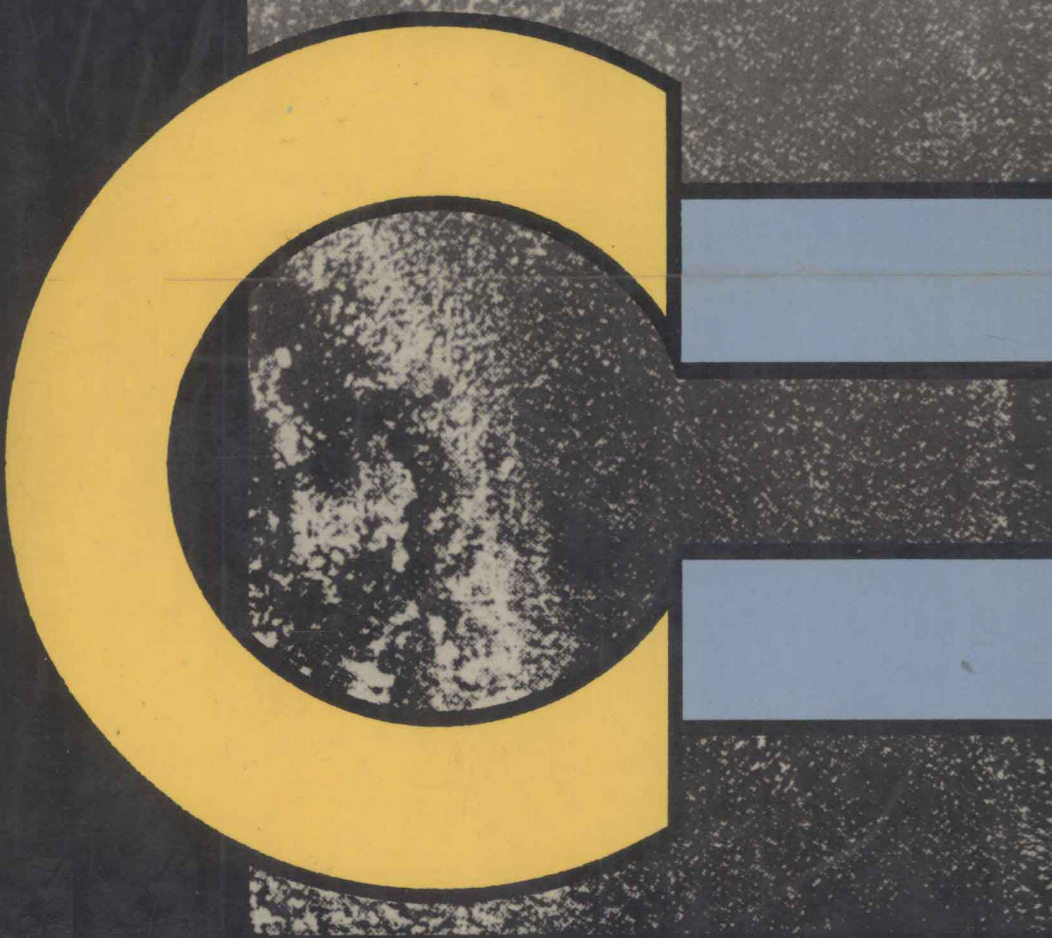
COMPUTER *Ethics*

Cautionary Tales and Ethical Dilemmas in Computing



TOM FORESTER

Computer Ethics

Cautionary Tales and Ethical Dilemmas in Computing

Tom Forester
and Perry Morrison

The MIT Press
Cambridge, Massachusetts

First MIT Press edition, 1990
Second printing, 1991

Published in the UK by Basil Blackwell, Oxford, England

Printed and bound in Great Britain.

Library of Congress Cataloging-in-Publication Data
Forester, Tom.
Computer ethics : cautionary tales and ethical dilemmas in computing / Tom Forester and Perry Morrison.
p. cm.
Includes bibliographical references.
ISBN 0-262-06131-7. – ISBN 0-262-56054-2 (pbk.)
1. Electronic data processing–Moral and ethical aspects.
I. Morrison, Perry. II. Title.
QA76.9.M65F67 1990b
174'.9004–dc20 89-71358 CIP

Computer Ethics

Also by Tom Forester

The Labour Party and the Working Class (1976)
The Microelectronics Revolution (ed.) (1980)
The Information Technology Revolution (ed.) (1985)
High-Tech Society (1987)
The Materials Revolution (ed.) (1988)
Computers in the Human Context (ed.) (1989)

Preface and Acknowledgements

The aim of this book is two-fold: (1) to describe some of the 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 arise, in turn, from two main sources: from hardware and software *malfunctions* and from *misuse* by human beings. We argue that computer systems by their very nature are 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. One lesson we quickly learned was that computer science students cannot be assumed to possess a social conscience or indeed have much awareness of social trends and global 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 courses are now including – or would like to include – an ethics component, but this noble objective has been hampered by a lack of suitable teaching materials. *Computer Ethics* has therefore been designed with teaching purposes in mind in an effort to help rectify the shortage of texts. That is why we have included numerous up-to-date references, as well as scenarios, role-playing exercises

and 'hypotheticals' in the suggestions for further discussion at the end of each chapter. The creative teacher should be able to build on these.

Readers will notice that we have not adopted an explicit theoretical framework and have avoided philosophical discussion of ethical theory. The reason is that this book is but a first step, with the simple aim of sensitizing undergraduate computer science students to ethical issues. Neither will readers find a detailed account of the legislative position around the world on the various topics discussed. This is because in each country the legal situation is often complex, confused and changing fast – 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 100 per cent reliable.

Tom Forester and Perry Morrison

Contents

1 Introduction: Our Computerized Society

Some Problems Created for Society by Computers – Ethical Dilemmas for Computer Professionals and Users

Computers are the core technology of our times. They are the new paradigm, the new 'common sense'. In the comparatively short space of 40 years, computers have become central to the operations of industrial societies. Without computers and their associated communication systems, much of manufacturing industry, commerce, transport and distribution, government, the military, health services, education and research would grind to a halt. Computers are certainly the most important technology to have come along this century and the current technological revolution may in time exceed the Industrial Revolution in terms of social significance. Our dependence upon computer and communication systems will grow still further as we enter the next millennium. Yet as society becomes more dependent on computers, we also become more and more vulnerable to computer malfunctions and to computer misuse – that is, to malfunctioning hardware and software and to misuse by human beings.

Some Problems Created for Society by Computers

The problems with computers and communications technology – commonly referred to jointly as 'information technology' (IT) – can be viewed in terms of scope, pervasiveness and complexity. First, information technology enables enormous quantities of information to be stored, retrieved and transmitted at great speed on a scale not possible before. This is all very well, but it has serious implications for data security and personal privacy (as well as employment) because computers are basically insecure. Second, information technology is permeating almost every aspect of our lives, including many areas previously untouched by technology. But unlike other pervasive technologies such as electricity, television and the motor car, computers are on the whole less reliable and less predictable

in their behaviour. Third, computer systems are often incredibly complex – so complex, in fact, that they are not always understood even by their creators. This often makes them completely unmanageable.

Unmanageable complexity can result in massive foul-ups or spectacular budget 'runaways': for example, Bank of America in 1988 had to abandon a $20 million computer system after spending five years and a further $60 million trying to make it work. Allstate Insurance has seen the cost of its new computer system rise from $8 million to a staggering $100 million and estimated completion delayed from 1987 to 1993. The Pentagon, the City of Richmond, the States of New Jersey and Oklahoma, Geophysical Systems Corp. and Blue Cross/Blue Shield of Wisconsin have all suffered major recent 'runaways'. Moreover, the problem seems to be getting worse: in 1988 the American Arbitration Association took on 190 computer disputes, most of which involved defective systems. The claims totalled $200 million – up from only $31 million in 1984.[1] Complexity can also result in disaster: no computer is 100 per cent guaranteed because it is virtually impossible to anticipate all sources of failure. Yet computers are regularly being used for all sorts of critical applications such as saving lives, flying aircraft, running nuclear power stations, transferring vast sums of money and controlling missile systems – and this can sometimes have tragic consequences.[2]

In fact, computers have figured one way or another in almost every famous system failure of recent times, 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, not to mention the sinking of *HMS Sheffield* in the Falklands' war and the shooting down of the Iranian airbus by the *USS Vincennes* over the Persian Gulf. Popular areas for computer malfunctions include telephone billing and telephone switching software, air traffic control systems, bank statements and bank teller machines, electronic funds transfer systems and motor vehicle licence databases, although industrial robots and police computers have contributed their fair share to the long list of foul-ups. Indeed, programming or design errors have resulted in the ozone hole at the South Pole remaining undetected for years, the failure of weather forecasters to predict Britain's Great Storm of October 1987 and the chaos in the 1986 Brazilian general election.[3] (Although computers have often taken the 'blame' on these occasions, the ultimate cause of failure in most cases is, in fact, human error.)

Every new technology creates new problems (as well as new benefits) for society and information technology is no exception. But digital computers have rendered society especially vulnerable to hardware and software malfunctions. Industrial robots go berserk while heart pacemakers and automatic garage door openers are rendered useless by 'electronic smog' emitted from point-of-sale terminals, personal computers and video

games.[4] Automated teller machines (ATMs), pumps at gas stations and fast-food outlet terminals are closed down because of unforeseen software snafus. It is reported that British businesses suffer around 30 major mishaps a year, involving losses running into millions of pounds. These are malfunctions caused by machine or human error and do not include human misuse in the form of fraud and sabotage. The cost of failures in domestically produced software in the UK alone is conservatively estimated at US $900 million per year.[5] In 1988, Dr John Collyer, a computer expert at the UK Ministry of Defence's Royal Signals and Radar Establishment (RSRE) warned that faulty microchips would start killing people in a big way within the next four years, while in 1989 a British Computer Society committee reported that much software was now so complex that current skills in safety assessment were inadequate and therefore the safety of people could not be guaranteed.[6]

Computers and communications technologies in turn are vulnerable to fires, floods, earthquakes and power cuts, as well as attacks from outside hackers and sabotage from inside employees. For example, a major fire which occurred in the Setagaya telephone office in Tokyo on 16 November 1984 destroyed 3,000 data communication and 89,000 ordinary telephone circuits resulting in total direct and indirect business losses of 13 billion yen.[7] In November 1987, a saboteur entered telecommunications tunnels in Sydney, Australia, and carefully severed 24 cables which knocked out 35,000 telephone lines in 40 Sydney suburbs, bringing down hundreds of computers, ATMs and POS, telex and fax terminals with it. Some businesses were completely out of action for 48 hours as engineers battled to restore services at a cost of thousands of dollars. Had the saboteur not been working with an out-of-date plan, the whole of Australia's telecommunications system could have been blacked out.[8]

In Chicago in 1986, a disgruntled employee at *Encyclopaedia Britannica*, angry at having been laid-off, merely tapped into the encyclopaedia's data base 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.'[9] A year later, another saboteur shut down the entire National Association of Securities Dealers' automatic quotation service (NASDAQ) for 82 minutes, keeping 20 million shares from being traded. The saboteur in question was an adventurous squirrel, who had caused a short circuit in Trumbull, Connecticut, where NASDAQ's main computer is situated. Meanwhile over in Denmark, a strike by 600 computer personnel paralysed that country's government for four months in 1986, causing the ruling party to call an early general election.[10]

The very existence of computers – and their ability to malfunction or to be abused – has created a whole new range of social problems or issues with which we need urgently to grapple. These include:

- the unauthorized use of hardware
- the theft of software
- disputed rights to products
- the use of computers to commit fraud
- the phenomenon of hacking and data theft
- sabotage in the form of viruses
- responsibility for the reliability of output (there is no warranty on software)
- making false claims for computers and
- the degradation of work.

Some of these issues are entirely new – in other instances, computers have merely created new versions of 'old' moral issues such as right and wrong, honesty, loyalty, responsibility, confidentiality and fairness. However, it is these issues which we intend to highlight in succeeding pages of this book.

Ethical Dilemmas for Computer Professionals and Users

Because computing is a relatively new and open field, the computer profession as such has had neither the time nor the organizational capability to establish a binding set of moral rules or ethics. Older professions, like medicine and the law, have had literally centuries to formulate their codes of conduct. And there is another problem, too: computer usage, unlike the practice of medicine or the law, goes outside the profession. We are all computer users now, and we are all to some extent faced with the same ethical dilemmas and conflicts of loyalty. Many of these dilemmas – like whether or not to copy software – are new 'grey areas' for which there is little in the way of accepted rules or social conventions, let alone established case law.

The ethical questions faced by computer professionals and computer users are numerous, but they include:

- Is copying software really a form of stealing? What sort of intellectual property rights should software developers have?
- Are so-called 'victimless' crimes (against, e.g., banks) more acceptable than crimes with human victims? Should computer professionals be sued for lax computer security?
- Is hacking merely a bit of harmless fun or is it a crime equivalent to burglary, forgery and/or theft?[11] Or are hackers to be seen as guardians of our civil liberties?

- Should the creation of viruses be considered deliberate sabotage and be punished accordingly?
- Does information on individuals stored in a computer constitute an intolerable invasion of privacy? How much protection are individuals entitled to?
- Who is responsible for computer malfunctions or errors in computer programs? Should computer companies be made to provide a warranty on software?
- Is 'artificial intelligence' a realistic and a proper goal for computer science? Should we trust our lives to allegedly artificially intelligent 'expert' systems?
- Should we allow the workplace to be computerized if it de-skills the workforce and/or increases depersonalization, fatigue and boredom?
- Is it OK for computer professionals to make false claims about the capabilities of computers when selling systems or representing computers to the general public? Is it ethical for computer companies to 'lock-in' customers to their products?
- Should, indeed, computer professionals be bound by a Code of Conduct and if so, what should it include?

In partial answer to the last question, the current state of play in the United States, for example, is that the Association for Computing Machinery (ACM) has a code of professional conduct; the Institute of Electrical and Electronics Engineers has adopted a code of ethics; the Data Processing Management Association (DPMA) also has a code of ethics; and the International Federation for Information Processing (IFIP) is in the process of developing one based on an international survey of opinion in the computing community. The British Computer Society (BCS) agreed codes of practice and conduct in 1983, while the Australian Computer Society (ACS) adopted a code of ethics in 1987.[12] In 1989, European computer societies, under the auspices of the Dutch Computer Society, began a process designed to formulate a Europe-wide code of practice. But it is fairly true to say that few of these worthy statements have or will have much force behind them, given that membership of these organizations is in general not compulsory. Enforcement is therefore difficult to non-existent.

One problem in developing ethical guidelines for the computer profession is that it does not have the status of professions like medicine or the law. Deborah G. Johnson, who has written extensively on the subject of computer ethics, likens the status of computer professionals to that of engineers. Mostly, she says, they work as employees rather than in their own right. While they have esoteric knowledge, they typically have quite limited autonomy. They often work in teams rather than alone and on small segments of large projects. They are usually distant from the effects

of their work and they do not have a single unifying and regulating professional organization. Like engineers, she says, they have four basic types of obligations:

1 obligations to society;
2 obligations to their employers;
3 obligations to their clients;
4 obligations to co-professionals and even professional organizations.

Conflicts can occur between every type of obligation (employer–client, employer–co-professionals, etc.), as well as within each category (e.g., between two different clients), but it is the conflict between computer professionals' obligations to their employer and their obligation to society that has received the most attention through the publicity given to 'whistle-blowing' cases.[13]

Yet despite their lower social status, the use of information technology for storing vital financial, marketing, personnel, health, research and military information puts new forms of power in the hands of computer professionals, from the humble operator to the top systems developer. This power is not specifically sought, but nevertheless computer professionals do find themselves in positions of power over employers, clients, co-professionals and the general public – and it is power which can be easily abused by those without scruples or those who easily fall victim to temptation.

Employers can be held to ransom by disgruntled employees who have the ability to change passwords or insert software 'time bombs' or 'logic bombs' which can knock out entire systems on a given date. For example, a programmer with a Minneapolis company was charged with extortion after threatening to trigger a 'time bomb' in the firm's computer system unless he received $350 per week until he found another job; a controversial DC government financial analyst changed the password to the Treasurer's office computer and refused to tell his superiors because he disagreed with their policies; and an employee of an Ontario company planted a 'logic bomb' in the company's computer designed to erase the entire system on a certain date – he was unhappy about a delayed salary increase.[14]

Clients are at the mercy of systems designers who alone know how a system works, consultants whose services may not strictly be necessary and computer companies who can virtually write their own bills. Society as a whole is vulnerable to the actions of computer professionals because most of the general public do not understand the dangers or implications of projects under the professionals' command. Because information is money and information is power, the information technology revolution has placed computer professionals under severe temptation: whether or not to abuse

this power of access to confidential and valuable information is one of the most important ethical dilemmas facing members of the new profession.

Computing educators therefore have a special responsibility to ensure that future generations of computer professionals are aware of the social problems caused by computers and are aware of the ethical conflicts they will face every day in their future roles as computer professionals. Tomorrow's graduates will also to some extent be considered 'experts' or spokespersons for the industry, interpreting computers to the wider world, and they will be creators of systems which will have major implications for organizations, the workplace and society in general.[15]

Computing educators should not merely be in the business of training technicians. They should be producing articulate information technologists – technologists endowed with communication skills, 'people skills' and possessing an appreciation of the social and ethical implications of information technology. They must prepare people for the messy real world, not the tidy, imaginary one inside a VDT screen.[16] They therefore have a duty to stimulate discussion about these issues and to generate awareness of the choices available to us. This book is a contribution to that task.

Notes

1 *Los Angeles Times*, 7 February 1988, p. 1 and *Los Angeles Times*, 29 June 1988 (from the ACM SIGSOFT's *Software Engineering Notes*, vol. 13, no. 3, July 1988, p. 4); articles by Jeffrey Rothfeder in *Business Week*, 7 November 1988 and 3 April 1989.

2 Peter Mellor, 'Can you count on computers?' *New Scientist*, 11 February 1989; David Bellin and Gary Chapman (eds), *Computers in Battle – Will They Work?* (Harcourt Brace Jovanovich, Boston, MA, 1987); Charles Perrow, *Normal Accidents: Living With High-Risk Technology* (Basic Books, New York, 1984).

3 *The New York Times*, 29 July 1986, p. C 1; *Computer News* (UK), 22 October 1987 and *New Scientist*, 3 March 1988; *Daily Telegraph*, 3 November 1986.

4 See, for example, Barry Fox, 'Electronic smog fouls the ether', *New Scientist*, 7 April 1988. For a more general discussion of vulnerability, see Jan Holvast, 'Vulnerability of information society', in Roger Clarke and Julie Cameron (eds), *Proceedings of SOST '89* (Australian Computer Society, Sydney, Australia, 1989).

5 *The Guardian*, 10 November 1986; Roger Woolnough, 'Britain scrutinizes software quality', *Electronics Engineering Times*, 13 June 1988.

6 *The Australian*, 2 February 1988 (reprinted from *The Times*); and *The Australian*, 21 February 1989.

7 Barry Fox, 'Corrupt power corrupts computer data', *New Scientist*, 29 October 1987; Katherine M. Hafner et al., 'Is your computer secure?' *Business Week*, 1 August 1988; Naruko Takanashi, Atsushi Tanaka, Hiroaki Yoshii and Yuji Wada, 'The Achilles' Heel of the information society: socioeconomic impacts of the telecommunication cable fire in the Setagaya Telephone Office, Tokyo', *Technological Forecasting and Social Change*, vol. 34, 1988, pp. 27–52.

8 'Saboteur tries to blank out Oz', *The Australian*, 23 November 1987, p. 1.

9 'Laid-off worker sabotages encyclopedia', *San Jose Mercury News*, 5 September 1986 (from *Software Engineering Notes*, vol. 11, no. 5, October 1986, p. 28).

10 'Stray rodent halts NASDAQ computers', *New York Times*, 10 December 1987, p. 33 and 'Computer strike forces Denmark poll', *The Australian*, August 20 1987 (from a UPI report).

11 In a recent court case in Britain, a 22 year-old hacker claimed that he had penetrated British Telecom's *Prestel* information system 'in order to make it more secure'. The prosecuting counsel replied: 'It's a bit like a burglar claiming all the credit for improved house security because the householder has put locks on the windows.' He claimed that the hacker was also guilty of forgery because he had used someone else's computer identification, which was 'equivalent to signing someone else's name without their consent' (*The Times*, London, 16 April 1986).

12 See Hal Sackman, 'Toward an IFIP code of ethics based on participative international consensus', in Roger Clarke and Julie Cameron (eds), *Proceedings of SOST '89*. For details of the BCS, DPMA, ACM and IEEE codes of ethics, see Deborah G. Johnson and John W. Snapper (eds), *Ethical Issues in the Use of Computers* (Wadsworth, Belmont, CA, 1985). For the others, contact the organizations concerned – indeed, this is advisable in all cases if up-to-date versions are required.

13 Unpublished paper by Deborah G. Johnson, 'The social responsibility of computer professionals', Department of Science and Technology Studies, Rensselaer Polytechnic Institute, Troy, NY, September 1988. See also a philosophical discussion of ethical theory in relation to computing in Deborah G. Johnson, *Computer Ethics* (Prentice-Hall, Englewood Cliffs, NJ, 1985); also Donn B. Parker, *Ethical Conflicts in Computer Science and Technology* (AFIPS Press/SRI International, Menlo Park, CA, 1981) and Donn B. Parker, Susan Swope and Bruce N. Baker, *Ethical Conflicts in Information and Computer Science, Technology and Business*, a report prepared for the National Science Foundation, Washington, DC, 1988); and W. Michael Hoffman and Jennifer Mills Moore (eds), *Ethics and the Management of Computer Technology* (Oelgeschlager, Gunn and Hain, Cambridge, MA, 1982).

14 *Minneapolis Star and Tribune*, 23 May 1985; *Washington Post*, 9 February 1986; *Globe and Mail*, Toronto, 3 November 1987.

15 For pleas along these lines, see Marcia Ascher, Ithaca College, Ithaca, NY, 'Ethical conflicts in the computing field: an undergraduate course', *Computers and Society*, vol. 16, no. 1, 1986; J. J. Buck BloomBecker, 'Computer ethics: an antidote to despair', *Computers and Society*, vol. 16, no. 4, 1986; Thomas J. De Loughry, 'Failure of colleges to teach computer ethics is called oversight with potentially catastrophic consequences', *The Chronicle of Higher Education*, 24 February 1988, p. A15; Delmar E. Searls, Asbury College, Wilmore, KY, 'Teaching computer ethics', *SIGCSE Bulletin*, vol. 20, no. 3, September 1988; and J. Daniel Couger, 'Preparing IS students to deal with ethical issues', *MIS Quarterly*, June 1989.

16 VDT (Visual Display Terminal) is used throughout this book rather than the UK expression VDU (Visual Display Unit) because it is the more common term in the rest of the world.