Ethics

for the information age

3rd edition

Michael J. Quinn
Seattle University

Boston San Francisco New York
London Toronto Sydney Tokyo Singapore Madrid
Mexico City Munich Paris Cape Town Hong Kong Montreal

Executive Editor Michael Hirsch
Senior Production Supervisor Marilyn Lloyd
Editorial Assistant Stephanie Sellinger
Cover Designer Barbara Atkinson
Text Designer Sandra Rigney
Cover Image © Al Francekevich/CORBIS
Marketing Manager Erin Davis
Project Management Windfall Software
Composition Windfall Software, using ZzTEX
Technical Illustration Laurel Muller, George Nichols
Copyeditor/Proofreader Richard Camp
Indexer Ted Laux
Rights and Permissions Advisor Dana Weightman
Senior Manufacturing Buyer Carol Melville
Printer Courier Stoughton, Inc.

Access the latest information about Addison-Wesley titles from our World Wide Web site:
http://www.aw-bc.com/computing

Library of Congress Cataloging-in-Publication Data

Ethics for the information age / Michael J. Quinn.—3rd ed.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-321-53685-3 (alk. paper)
ISBN-10: 0-321-53685-1 (alk. paper)
1. Electronic data processing—Moral and ethical aspects. 2. Computers and civilization. I. Quinn, Michael J. (Michael Jay)
QA76.9.M65Q56 2008
174′.9004—dc22

2007052271

ISBN 13: 9780321536853
ISBN 10: 0-321-53685-1
3 4 5 6 7 8 9 10—CRS—11 10 09

CHAPTER

8 Professional Ethics

We have come through a strange cycle in programming, starting with the creation of programming itself as a human activity. Executives with the tiniest smattering of knowledge assume that anyone can write a program, and only now are programmers beginning to win their battle for recognition as true professionals.

–GERALD WEINBERG, *The Psychology of Computer Programming*, 1971

8.1 Introduction

INFORMALLY, A **PROFESSION** IS A VOCATION THAT REQUIRES A HIGH LEVEL OF EDUCATION and practical experience in the field. Medicine and law are two well-known professions. We pay doctors and lawyers well, trusting that they will correctly ascertain and treat our medical and legal problems, respectively. Professionals have a special obligation to ensure their actions are for the good of those who depend on them because their decisions can have more serious consequences than the choices made by those holding less responsible positions in society.

In this chapter we focus on moral decisions made by people who design, implement, or maintain computer hardware or software systems. We begin by considering the extent to which a computer-related career is a profession along the lines of medicine or law. Next, we present and analyze a code of ethics for an important computer-related discipline: software engineering. Our analysis leads us into a discussion of virtue ethics,

an ethical theory based on the idea that good character is the source of correct moral decisions. Three case studies give us the opportunity to use the software engineering code of ethics as a tool for ethical analysis.

Finally, we discuss whistleblowing: a situation in which a member of an organization breaks ranks to reveal actual or potential harm to the public. Whistleblowing raises important moral questions about loyalty, trust, and responsibility. Two accounts of whistleblowing illuminate these moral questions and demonstrate the personal sacrifices some have made for the greater good of society. We consider the important role management plays in creating an organizational atmosphere that either allows or suppresses internal dissent.

8.2 Are Computer Experts Professionals?

Millions of people have a computer-related job title, such as computer engineer, computer scientist, programmer, software engineer, system administrator, or systems analyst. Is a computer-related career a profession like medicine or law? Let's consider the characteristics of a well-developed profession.

8.2.1 Characteristics of a Profession

A fully developed profession has a well-organized infrastructure for certifying new members and supporting those who already belong to the profession. Ford and Gibbs have identified eight components of a mature professional infrastructure [1]:

- *Initial professional education*—formal course work completed by candidates before they begin practicing the profession
- *Accreditation*—assures that the formal course work meets the standards of the profession
- *Skills development*—activities that provide candidates with the opportunity to gain practical skills needed to practice the profession
- *Certification*—process by which candidates are evaluated to determine their readiness to enter the profession
- *Licensing*—the process giving candidates the legal right to practice the profession
- *Professional development*—formal course work completed by professionals in order to maintain and develop their knowledge and skills
- *Code of ethics*—mechanism by which a profession ensures that its members will use their knowledge and skills for the benefit of society
- *Professional society*—organization promoting the welfare of the profession, typically consisting of most if not all of the members of the profession

Figure 8.1 illustrates how these components work together to support the profession. A person desiring to join the profession undertakes some initial professional education. A process of accreditation assures that the educational process is sound. After

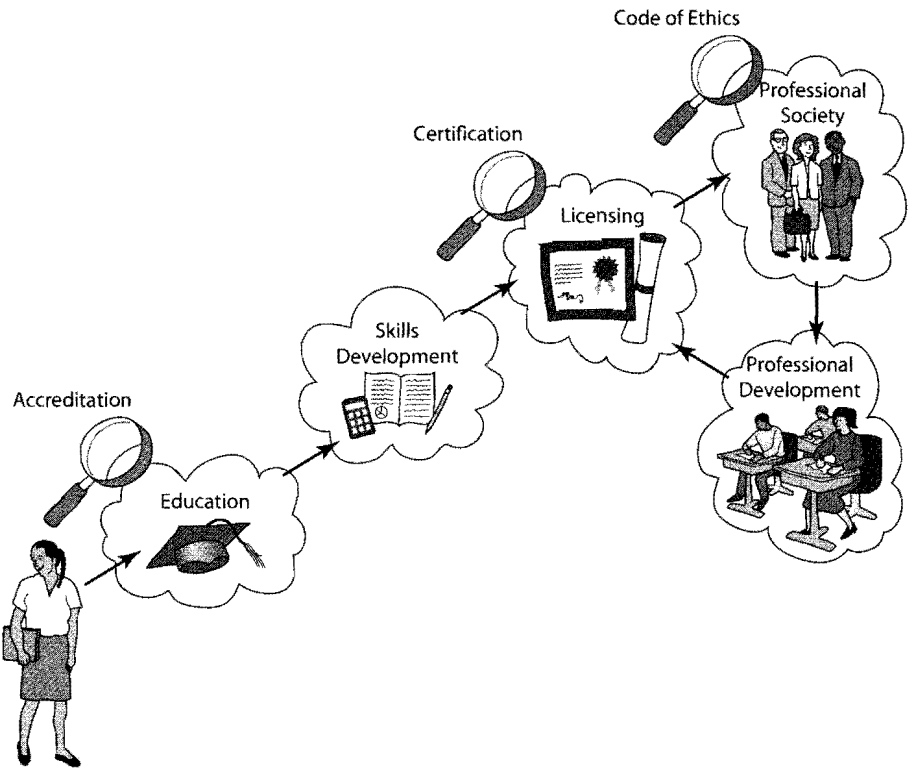

Figure 8.1 A mature profession has eight attributes that enable it to certify new members and support existing members [1].

completing their formal education, candidates gain skills through practical experience working in the field. Another check determines if the candidate is ready to be certified. Successful candidates are licensed to practice the profession.

When the public can trust the competence and integrity of the members of a profession, every one of its members benefits. For this reason professionals have a stake in ensuring that fellow members of the profession are capable and act appropriately. For mature professions, professional societies establish codes of ethics and require their members to keep their knowledge current through continuing education and training. Professionals who do not follow the code of ethics or fail to keep up with changes in the field can lose their licenses.

8.2.2 Certified Public Accountants

To illustrate these steps, let's consider how a person becomes a Certified Public Accountant (CPA). We choose accounting because it is a fully developed profession that does

not require graduate study for membership. In this respect it is more similar to a typical computer-related career than the medical or legal professions, which require their members to earn advanced degrees.

The first step for someone wishing to become a CPA is to graduate with 150 semester credit hours and at least a bachelor's degree from an accredited college or university. Many people pursuing a CPA choose to major in accounting, although it is not strictly necessary. However, the candidate must have completed at least 24 semester credit hours in accounting, auditing, business law, finance, and tax subjects.

After graduation, the candidate gets practical training in the profession by finding employment as an accountant working under the supervision of a CPA.

Finally, candidates must sit for the CPA exam, which has four sections. Candidates who do not pass at least two parts must re-take the entire exam. Candidates who pass at least two parts of the exam must pass the remaining parts within five years.

Completion of the necessary formal education, plus satisfactory scores on every section of the CPA exam, plus two years' work experience enable an accountant to become a Certified Public Accountant. In order to retain certification, CPAs must fulfill continuing education requirements and abide by the profession's code of ethics.

8.2.3 Computer-Related Careers

IS A COMPUTER-RELATED CAREER A PROFESSION?

It is easy to find a crucial difference between system analysts, computer programmers, and system administrators on the one hand and accountants, lawyers, and physicians on the other hand. At the heart of every mature profession is certification and licensing. Certification and licensing allow a profession to determine who will be allowed to practice the profession. For example, a person may not practice law in a state without passing the bar exam and being granted a license. In contrast, people may write computer programs and maintain computer systems, either as consultants, sole proprietors, or members of larger firms, without being certified or having been granted a license.

Without certification and licensing, the rest of the characteristics of a mature profession become irrelevant. A person does not have to complete college or serve an apprenticeship under the guidance of an experienced mentor in order to gain employment as a programmer, system administrator, or systems analyst. The vast majority of people who hold computer-related jobs do not belong to either of computing's professional societies. It is up to particular employers to monitor the behavior of their employees and guide their continuing education—no professional organization has the authority to forbid someone from managing computer networks or writing computer programs.

In another important respect computer programmers differ from most professionals, such as dentists and ministers. Typically, professionals work directly with individual clients. A dentist treats one patient at a time. An accountant audits one business at a time. Most computer programmers work inside a company as part of a team that includes many other programmers as well as managers. In this environment the responsibility of an individual person is more difficult to discern. Low-level technical decisions are made by groups, and final authority rests with management.

STATUS OF CERTIFICATION AND LICENSING

The two largest organizations supporting the computing field are the IEEE Computer Society (IEEE-CS), with about 90,000 members, and the Association for Computing Machinery (ACM), with about 63,000 members. Like organizations supporting mature professions, the IEEE-CS and the ACM strive to advance the discipline and support their members through publications, conferences, local chapters, student chapters, technical committees, and the development of standards.

A software engineer is someone engaged in the development or maintenance of software, or someone who teaches in this area. In 1993 the IEEE-CS and ACM set up a joint steering committee to explore the establishment of software engineering as a profession. The joint steering committee created several task forces to address particular issues. One task force conducted a survey of practitioners with the goal of understanding the knowledge and skills required by software engineers. Another task force developed accreditation criteria for undergraduate programs in software engineering. A third task force developed a code of ethics for software engineers.

In May 1999 the ACM Council passed a resolution that stated, in part, "ACM is opposed to the licensing of software engineers at this time because ACM believes that it is premature and would not be effective in addressing the problems of software quality and reliability" [2].

ABILITY TO HARM PUBLIC

In one key respect—the ability to harm members of the public—those who design, implement, and maintain computer hardware and software systems sometimes hold responsibilities similar to those held by members of mature professions. The Therac-25 killed or gravely injured at least six people, in part because of defective software. While most software engineers do not write code for safety-critical systems such as linear accelerators, society does depend on the quality of their work. People make important business decisions based on the results they get from their spreadsheet programs. Millions rely upon commercial software to help them produce their income tax returns. Errors in programs can result in such harms as lost time, incorrect businesses decisions, and fines. System administrators are responsible for keeping computer systems running reliably without infringing on the privacy of the computer users.

The ability to cause harm to members of the public is a powerful reason why those in computer-related careers should follow a code of ethics, even if they are not professionals in the same sense as physicians, lawyers, and CPAs. As a good example of a code of ethics for those in computer-related disciplines, we present the Software Engineering Code of Ethics and Professional Practice, endorsed by both the ACM and the IEEE-CS.

8.3 Software Engineering Code of Ethics

The Software Engineering Code of Ethics and Professional Practice is a practical framework for moral decision making related to problems that software engineers may encounter.

8.3.1 Preamble

Computers have a central and growing role in commerce, industry, government, medicine, education, entertainment and society at large. Software engineers are those who contribute by direct participation or by teaching, to the analysis, specification, design, development, certification, maintenance and testing of software systems. Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice.

The Code contains eight Principles related to the behavior of and decisions made by professional software engineers, including practitioners, educators, managers, supervisors and policymakers, as well as trainees and students of the profession. The Principles identify the ethically responsible relationships in which individuals, groups, and organizations participate and the primary obligations within these relationships. The Clauses of each Principle are illustrations of some of the obligations included in these relationships. These obligations are founded in the software engineer's humanity, in special care owed to people affected by the work of software engineers, and the unique elements of the practice of software engineering. The Code prescribes these as obligations of anyone claiming to be or aspiring to be a software engineer.

It is not intended that the individual parts of the Code be used in isolation to justify errors of omission or commission. The list of Principles and Clauses is not exhaustive. The Clauses should not be read as separating the acceptable from the unacceptable in professional conduct in all practical situations. The Code is not a simple ethical algorithm that generates ethical decisions. In some situations standards may be in tension with each other or with standards from other sources. These situations require the software engineer to use ethical judgment to act in a manner which is most consistent with the spirit of the Code of Ethics and Professional Practice, given the circumstances.

Ethical tensions can best be addressed by thoughtful consideration of fundamental principles, rather than blind reliance on detailed regulations. These Principles should influence software engineers to consider broadly who is affected by their work; to examine if they and their colleagues are treating other human beings with due respect; to consider how the public, if reasonably well informed, would view their decisions; to analyze how the least empowered will be affected by their decisions; and to consider whether their acts would be judged worthy of the ideal professional working as a software engineer. In all these judgments concern for the health, safety and welfare of the public is primary; that is, the "Public Interest" is central to this Code.

The dynamic and demanding context of software engineering requires a code that is adaptable and relevant to new situations as they occur. However, even in this generality, the Code provides support for software engineers and managers of software engineers who need to take positive action in a specific case by documenting the ethical stance of the profession. The Code provides an ethical foundation to which individuals within teams and the team as a whole can appeal. The Code helps to define those actions that are ethically improper to request of a software engineer or teams of software engineers.

The Code is not simply for adjudicating the nature of questionable acts; it also has an important educational function. As this Code expresses the consensus of the profession on ethical issues, it is a means to educate both the public and aspiring professionals about the ethical obligations of all software engineers.

8.3.2 Principles

PRINCIPLE 1: PUBLIC

Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:

1.01 Accept full responsibility for their own work.

1.02 Moderate the interests of the software engineer, the employer, the client and the users with the public good.

1.03 Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish

FIGURE 8.2 Software engineers shall approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy, or harm the environment. The ultimate effect of the work should be to the public good (Clause 1.03).

privacy or harm the environment. The ultimate effect of the work should be to the public good.

1.04 Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.

1.05 Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.

1.06 Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.

1.07 Consider issues of physical disabilities, allocation of resources, economic disadvantage and other factors that can diminish access to the benefits of software.

1.08 Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.

PRINCIPLE 2: CLIENT AND EMPLOYER

Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest. In particular, software engineers shall, as appropriate:

2.01 Provide service in their areas of competence, being honest and forthright about any limitations of their experience and education.

2.02 Not knowingly use software that is obtained or retained either illegally or unethically.

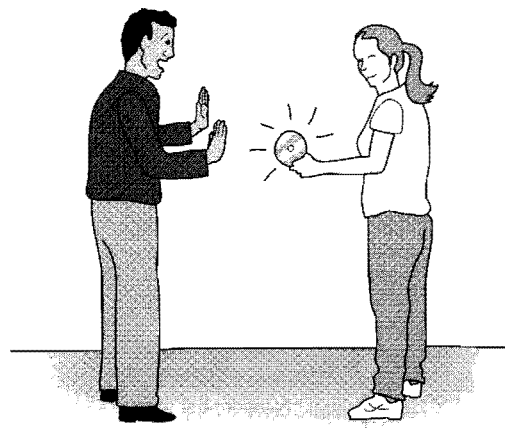

FIGURE 8.3 Software engineers shall not knowingly use software that is obtained or retained either illegally or unethically (Clause 2.02).

2.03 Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.

2.04 Ensure that any document upon which they rely has been approved, when required, by someone authorized to approve it.

2.05 Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law.

2.06 Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.

2.07 Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.

2.08 Accept no outside work detrimental to the work they perform for their primary employer.

2.09 Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.

PRINCIPLE 3: PRODUCT

Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. In particular, software engineers shall, as appropriate:

3.01 Strive for high quality, acceptable cost and a reasonable schedule, ensuring significant tradeoffs are clear to and accepted by the employer and the client, and are available for consideration by the user and the public.

3.02 Ensure proper and achievable goals and objectives for any project on which they work or propose.

3.03 Identify, define and address ethical, economic, cultural, legal and environmental issues related to work projects.

3.04 Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.

3.05 Ensure an appropriate method is used for any project on which they work or propose to work.

3.06 Work to follow professional standards, when available, that are most appropriate for the task at hand, departing from these only when ethically or technically justified.

3.07 Strive to fully understand the specifications for software on which they work.

3.08 Ensure that specifications for software on which they work have been well documented, satisfy the users' requirements and have the appropriate approvals.

FIGURE 8.4 Software engineers shall ensure proper and achievable goals and objectives for any project on which they work or propose (Clause 3.02).

3.09 Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work and provide an uncertainty assessment of these estimates.

3.10 Ensure adequate testing, debugging, and review of software and related documents on which they work.

3.11 Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.

3.12 Work to develop software and related documents that respect the privacy of those who will be affected by that software.

3.13 Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.

3.14 Maintain the integrity of data, being sensitive to outdated or flawed occurrences.

3.15 Treat all forms of software maintenance with the same professionalism as new development.

PRINCIPLE 4: JUDGMENT

Software engineers shall maintain integrity and independence in their professional judgment. In particular, software engineers shall, as appropriate:

4.01 Temper all technical judgments by the need to support and maintain human values.

4.02 Only endorse documents either prepared under their supervision or within their areas of competence and with which they are in agreement.

4.03 Maintain professional objectivity with respect to any software or related documents they are asked to evaluate.

4.04 Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

4.05 Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

4.06 Refuse to participate, as members or advisors, in a private, governmental or professional body concerned with software related issues, in which they, their employers or their clients have undisclosed potential conflicts of interest.

PRINCIPLE 5: MANAGEMENT

Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance. In particular, those managing or leading software engineers shall, as appropriate:

5.01 Ensure good management for any project on which they work, including effective procedures for promotion of quality and reduction of risk.

5.02 Ensure that software engineers are informed of standards before being held to them.

5.03 Ensure that software engineers know the employer's policies and procedures for protecting passwords, files and information that is confidential to the employer or confidential to others.

5.04 Assign work only after taking into account appropriate contributions of education and experience tempered with a desire to further that education and experience.

5.05 Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work, and provide an uncertainty assessment of these estimates.

5.06 Attract potential software engineers only by a full and accurate description of the conditions of employment.

5.07 Offer fair and just remuneration.

5.08 Not unjustly prevent someone from taking a position for which that person is suitably qualified.

5.09 Ensure that there is a fair agreement concerning ownership of any software, processes, research, writing, or other intellectual property to which a software engineer has contributed.

5.10 Provide for due process in hearing charges of violation of an employer's policy or of this Code.

5.11 Not ask a software engineer to do anything inconsistent with this Code.

5.12 Not punish anyone for expressing ethical concerns about a project.

FIGURE 8.5 Software engineers shall help develop an organizational environment favorable to acting ethically (Clause 6.01).

PRINCIPLE 6: PROFESSION

Software engineers shall advance the integrity and reputation of the profession consistent with the public interest. In particular, software engineers shall, as appropriate:

6.01 Help develop an organizational environment favorable to acting ethically.

6.02 Promote public knowledge of software engineering.

6.03 Extend software engineering knowledge by appropriate participation in professional organizations, meetings and publications.

6.04 Support, as members of a profession, other software engineers striving to follow this Code.

6.05 Not promote their own interest at the expense of the profession, client or employer.

6.06 Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

6.07 Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.

6.08 Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

6.09 Ensure that clients, employers, and supervisors know of the software engineer's commitment to this Code of ethics, and the subsequent ramifications of such commitment.

6.10 Avoid associations with businesses and organizations which are in conflict with this code.

6.11 Recognize that violations of this Code are inconsistent with being a professional software engineer.

6.12 Express concerns to the people involved when significant violations of this Code are detected unless this is impossible, counter-productive, or dangerous.

6.13 Report significant violations of this Code to appropriate authorities when it is clear that consultation with people involved in these significant violations is impossible, counter-productive or dangerous.

PRINCIPLE 7: COLLEAGUES

Software engineers shall be fair to and supportive of their colleagues. In particular, software engineers shall, as appropriate:

7.01 Encourage colleagues to adhere to this Code.

7.02 Assist colleagues in professional development.

7.03 Credit fully the work of others and refrain from taking undue credit.

7.04 Review the work of others in an objective, candid, and properly documented way.

7.05 Give a fair hearing to the opinions, concerns, or complaints of a colleague.

7.06 Assist colleagues in being fully aware of current standard work practices including policies and procedures for protecting passwords, files and other confidential information, and security measures in general.

7.07 Not unfairly intervene in the career of any colleague; however, concern for the employer, the client or public interest may compel software engineers, in good faith, to question the competence of a colleague.

7.08 In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

PRINCIPLE 8: SELF

Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession. In particular, software engineers shall continually endeavor to:

8.01 Further their knowledge of developments in the analysis, specification, design, development, maintenance and testing of software and related documents, together with the management of the development process.

8.02 Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.

8.03 Improve their ability to produce accurate, informative, and well-written documentation.

8.04 Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.

8.05 Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.

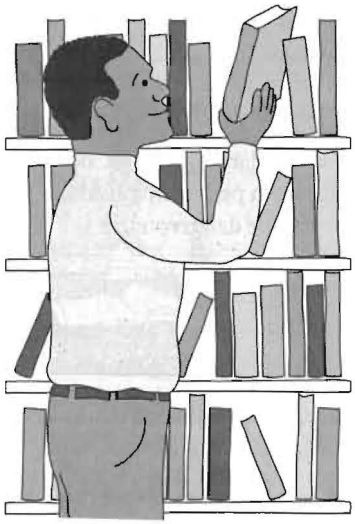

FIGURE 8.6 Software engineers shall continually endeavor to improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time (Clause 8.02).

8.06 Improve their knowledge of this Code, its interpretation, and its application to their work.

8.07 Not give unfair treatment to anyone because of any irrelevant prejudices.

8.08 Not influence others to undertake any action that involves a breach of this Code.

8.09 Recognize that personal violations of this Code are inconsistent with being a professional software engineer.

8.4 Analysis of the Code

In this section we analyze the Code and derive an alternate set of underlying principles upon which it rests.

8.4.1 Preamble

The preamble to the Code points out that there is no mechanical process for determining the correct actions to take when faced with a moral problem. Our experience evaluating moral problems related to the introduction and use of information technology confirms this statement. Even two people with similar philosophies may reach different conclusions when confronted with a moral problem. Two Kantians may agree on the basic facts of a moral problem, but disagree on how to characterize the will of the moral agent. Two utilitarians may agree on the benefits and harms resulting from a proposed action, but assign different weights to the outcomes, causing them to reach opposite conclusions.

The preamble also warns against taking an overly legalistic view of the Code. Simply because an action is not expressly forbidden by the Code does not mean it is morally acceptable. Instead, judgment is needed to detect when a moral problem has arisen and to determine the right thing to do in a particular situation.

While the Code is expressed as a collection of rules, these rules are based on principles grounded in different ethical theories. This is not surprising, considering that the Code was drafted by a committee. When we encounter a situation where two rules conflict, the preamble urges us to ask questions that will help us consider the principles underlying the rules. These questions demonstrate the multifaceted grounding of the Code:

1. *Who is affected?*

   Utilitarians focus on determining how an action benefits or harms other people.

2. *Am I treating other human beings with respect?*

   Kant's Categorical Imperative tells us to treat others as ends in themselves, rather than simply as a means to an end.

3. *Would my decision hold up to public scrutiny?*

   A cultural relativist is concerned about whether an action conforms with the mores of society.

4. *How will those who are least empowered be affected?*

   Rawls's second principle of justice requires us to consider whether inequalities are to the greatest benefit of the least-advantaged members of society.

5. *Are my acts worthy of the ideal professional?*

   The ethics of virtue is based on imitation of morally superior role models. Since we did not discuss virtue ethics in Chapter 2, let's examine it now.

8.4.2 Virtue Ethics

ORIGIN OF VIRTUE ETHICS

In *The Nicomachean Ethics*, Aristotle expresses the opinion that happiness results from living a life of virtue [3]. He distinguishes between *intellectual virtue*, which is developed through education, and *moral virtue*, which comes about through repetition of the appropriate acts (Figure 8.7). You can acquire the virtue of honesty, for example, by habitually telling the truth. According to Aristotle, deriving pleasure from a virtuous act is a sign that you have acquired that virtue.

There is a wealth of virtues, of course. Here is a brief list of two dozen virtues given by James Rachels: benevolence, civility, compassion, conscientiousness, cooperativeness, courage, courteousness, dependability, fairness, friendliness, generosity, honesty, industriousness, justice, loyalty, moderation, patience, prudence, reasonableness, self-discipline, self-reliance, tactfulness, thoughtfulness, and tolerance [4].

A person who possesses many moral virtues has a strong moral character. According to Aristotle, when people with strong character face a moral problem, they know the

FIGURE 8.7 According to Aristotle, happiness derives from living a life of virtue. You acquire moral virtues by repeating the appropriate acts.

right thing to do, because the action will be consistent with their character. As Justin Oakley and Dean Cocking put it, "An action is right if and only if it is what an agent with a virtuous character would do in the circumstances" [5].

STRENGTHS OF VIRTUE ETHICS

Virtue ethics has two advantages over the ethical theories we considered in Chapter 2. First, it provides a motivation for good behavior. The calculus of utility and the Categorical Imperative say nothing about motivation. A utilitarian or a Kantian may do the right thing, but the reasoning behind the action is cold and analytical. Virtue ethics, on the other hand, stresses the importance of loyalty, thoughtfulness, courteousness, dependability, and other characteristics of healthy social interactions.

A second advantage of virtue ethics is that it provides a solution to the problem of impartiality. Recall that utilitarianism, Kantianism, and social contract theory require us to be completely impartial and treat all human beings as equals. This assumption leads to moral evaluations that are hard for most people to accept. For example, when a couple is faced with the choice between using $4,000 to take their children to Disneyland for a week or feeding 1,000 starving Africans for a month, the calculus of utility would conclude saving 1,000 lives was the right thing to do. However, most of us expect that good parents will show more kindness to their children than to people living on the other side of the world.

Virtue ethics avoids the pitfall of impartiality by rejecting the notion that every action must be designed to produce the maximum benefit for people overall [5]. Instead, some virtues are partial toward certain people, while others are impartial and treat everyone equally. Love, friendship, and loyalty are examples of virtues that allow a person to be partial toward friends and family members. Honesty, civility, and courteousness are examples of virtues that a person would extend equally to all human beings.

WEAKNESS OF VIRTUE ETHICS

However, virtue ethics has a significant liability. Using virtue ethics alone, it is often difficult to determine what to do in a particular situation. Suppose you are in charge of dispatching crews to fight brush fires in southern California. Three fires erupt at the same time: one near a mountain resort frequented by the wealthy; another near a town of 10,000 people with a high rate of poverty; and a third close to a middle-class suburb. You only have the resources to fight two of the fires. Which fires do you attack? Looking back on the list of virtues, which ones come into play? Compassion? Fairness? Justice? Prudence?

Suppose we decide the most relevant virtue is prudence. What is the prudent thing to do? Perhaps prudence dictates that you allocate fire crews to minimize property damage, but making your decision based on the total value of the property that each fire is threatening is an example of the utilitarian approach to moral problem solving.

Perhaps the most relevant virtue is justice. Suppose only two of the fires are inside the fire-control district that funds the fire-fighting brigade. Using justice as your virtue, you may decide to abide by the fire district policies. Following written policies looks suspiciously like a Kantian approach to decision making.

You may argue that the desire to be prudent came before the decision to take a utilitarian approach, or the will to be just was an antecedent to a Kantian analysis. Even if this were so, a fundamental problem remains. If the desire to exercise different virtues compels you toward different actions, which action should you take? Put another way, what is the methodology for answering the question, "What would a person with strong moral character do in these circumstances?"

VIRTUE ETHICS COMPLEMENTS OTHER THEORIES

Rather than treating virtue ethics as a stand-alone theory, some ethicists believe it makes more sense to see virtue ethics as a complement to one of the other theories, such as utilitarianism. Adding virtue ethics allows ethical decision makers to consider their rationale for taking the action as well as the beneficial or harmful effects of the action.

Remember the problem of moral luck, one of the major criticisms of act utilitarianism? Since an action is judged right or wrong based solely on its consequences, an unlucky, unintended consequence can result in an action being considered wrong. Suppose your mother-in-law is in the hospital and you send her an expensive and beautiful bouquet of flowers. Unfortunately, she gets an allergic reaction to one of the flowers in the bouquet. As a result, she must spend an additional four days in the hospital. From a

purely act utilitarian point of view, you did the wrong thing when you sent your mother-in-law the flowers. In a mixed act utilitarian/virtue ethics theory, we would also take into account that you were acting out of thoughtfulness, a virtue. If nothing else, introducing the virtue ethics component makes it easier for us to think about some of the other consequences of the action. Despite the allergic reaction, your mother-in-law appreciated your kind gesture, a benefit. In addition, you strengthened your habit of thoughtfulness by practicing it on your mother-in-law, another benefit.

8.4.3 Alternative List of Fundamental Principles

The start of each section of the Code begins with the statement of a fundamental principle. For example, the first section begins with the fundamental principle, "Software engineers shall act consistently with the public interest." All of these statements of fundamental principles are expressed from the point of view of what software engineers ought to do.

Another way to devise a list of fundamental principles is to consider those virtues we would like to instill among all the members of any profession. We end up with a set of general, discipline-independent rules that cut across the eight categories of the Code. Here is an alternative list of fundamental principles derived using that approach:

1. *Be impartial.*

   The good of the general public is equally important to the good of your organization or company. The good of your profession and your company are equally important to your personal good. It is wrong to promote your agenda at the expense of your firm, and it is wrong to promote the interests of your firm at the expense of society. (Supports Clauses 1.02, 1.03, 1.05, 1.07, 3.03, 3.12, 4.01, and 6.05.)

2. *Disclose information that others ought to know.*

   Do not let others come to harm by concealing information from them. Do not make misleading or deceptive statements. Disclose potential conflicts of interest. (Supports Clauses 1.04, 1.06, 2.06, 2.07, 3.01, 4.05, 4.06, 5.05, 5.06, 6.07, 6.08, 6.09, 6.12, and 6.13.)

3. *Respect the rights of others.*

   Do not infringe on the privacy rights, property rights, or intellectual property rights of others. (Supports Clauses 2.02, 2.03, 2.05, and 3.13.)

4. *Treat others justly.*

   Everyone deserves fair wages and appropriate credit for work performed. Do not discriminate against others for attributes unrelated to the job they must do. Do not penalize others for following the Code. (Supports Clauses 5.06, 5.07, 5.08, 5.09, 5.10, 5.11, 5.12, 7.03, 7.04, 7.05, 7.07, and 8.07.)

5. *Take responsibility for your actions and inactions.*

   As a moral agent, you are responsible for the things you do, both good and bad. You may also be responsible for bad things that you allow to happen through your

inaction. (Supports Clauses 1.01, 3.04, 3.05, 3.06, 3.07, 3.08, 3.10, 3.11, 3.14, 3.15, 4.02, and 7.08.)

6. *Take responsibility for the actions of those you supervise.*

   Managers are responsible for setting up work assignments and training opportunities to promote quality and reduce risk. They should create effective communication channels with subordinates so that they can monitor the work being done and be aware of any quality or risk issues that arise. (Supports Clauses 5.01, 5.02, 5.03, and 5.04.)

7. *Maintain your integrity.*

   Deliver on your commitments and be loyal to your employer, while obeying the law. Do not ask someone else to do something you would not be willing to do yourself. (Supports Clauses 2.01, 2.04, 2.08, 2.09, 3.01, 3.02, 3.09, 4.03, 4.04, 6.06, 6.10, 6.11, 8.08, and 8.09.)

8. *Continually improve your abilities.*

   Take advantage of opportunities to improve your software engineering skills and your ability to put the Code to use. (Supports Clauses 8.01, 8.02, 8.03, 8.04, 8.05, and 8.06.)

9. *Share your knowledge, expertise, and values.*

   Volunteer your time and skills to worthy causes. Help bring others to your level of knowledge about software engineering and professional ethics. (Supports Clauses 1.08, 6.01, 6.02, 6.03, 6.04, 7.01, 7.02, and 7.06.)

In the following section we will use these fundamental principles to guide our analysis in three case studies.

8.5 Case Studies

Throughout this text we have evaluated a wide range of moral problems. Our methodology has been to evaluate the moral problem from the point of view of Kantianism, act utilitarianism, rule utilitarianism, and social contract theory.

Another way to evaluate information technology–related moral problems is to make use of the Software Code of Ethics and Professional Practice. We follow a three-step process:

1. Consult the list of fundamental principles and identify those that are relevant to the moral problem.
2. Search the list of clauses accompanying each of the relevant fundamental principles to see which speak most directly to the issue.
3. Determine whether the contemplated action aligns with or contradicts the statements in the clauses. If the action is in agreement with all of the clauses, that provides strong evidence the action is moral. If the action is in disagreement with all of the clauses, it is safe to say the action is immoral.

Usually, the contemplated action will be supported by some clauses and opposed by others. When this happens, we must use our judgment to determine which of the clauses are most important before we can reach a conclusion about the morality of the contemplated action.

In the remainder of this section we will apply this methodology to three case studies.

8.5.1 Software Recommendation

SCENARIO

Sam Shaw calls the Department of Computer Science at East Dakota State University seeking advice on how to improve the security of his business's local area network. A secretary in the department routes Mr. Shaw's call to Professor Jane Smith, an internationally recognized expert in the field. Professor Smith answers several questions posed by Mr. Shaw regarding network security. When Mr. Shaw asks Professor Smith to recommend a software package to identify security problems, Professor Smith tells him that NetCheks got the personal computer magazine's top rating. She does not mention that the same magazine gave a "best buy" rating to another product with fewer features but a much lower price. She also fails to mention that NetCheks is a product of a spin-off company started by one of her former students and that she owns 10 percent of the company.

Analysis

From our list of nine fundamental principles, three are most relevant here:

- Be impartial.
- Disclose information that others ought to know.
- Share your knowledge, expertise, and values.

Searching the list of clauses identified with these fundamental principles, the following ones seem to fit the case study most closely:

- *1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.*
  Professor Smith was deceptive when she mentioned the most highly rated software package but not the one rated to be a "best buy."
- *1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.*
- *6.02. Promote public knowledge of software engineering.*
  Professor Smith freely provided Sam Shaw with valuable information about network security.
- *4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.*
- *6.05. Not promote their own interest at the expense of the profession, client or employer.*

Professor Smith did not tell Sam Shaw that she had a personal stake in the success of the NetCheks software. She did not tell him about the "best buy" package that may have provided him every feature he needed at a much lower price.

Mr. Shaw was asking Professor Smith for free advice, and she provided it. When she freely shared her knowledge about network security, she was acting in the spirit of Clauses 1.08 and 6.02, and doing a good thing.

However, Professor Smith appears to have violated the other three clauses to at least some degree. Most importantly, she did not reveal her personal interest in NetCheks, which could lead her to be biased. The fact that the she did not mention the "best buy" package is evidence that she was neither evenhanded nor completely forthcoming when she answered Mr. Shaw's question about software packages.

Perhaps Mr. Shaw should have heeded the maxim "Free advice is worth what you pay for it." Nevertheless, the ignorance or foolishness of one person does not excuse the bad behavior of another. Professor Smith should have revealed her conflict of interest. At that point, Mr. Shaw could have chosen to get another opinion, if he so desired. ≈

8.5.2 Child Pornography

≈ Scenario

Joe Green, a system administrator for a large corporation, is installing a new software package on the PC used by employee Chuck Dennis. The company has not authorized Joe to read other people's emails, Web logs, or personal files. However, in the course of installing the software he accidentally comes across directories containing files with suspicious-looking names. He opens a few of the files and discovers they contain child pornography. Joe believes possessing such images is against federal law. What should he do?

Analysis

Looking over the list of nine fundamental principles, we find these to be most relevant to our scenario:

- Be impartial
- Respect the rights of others.
- Treat others justly.
- Maintain your integrity.

We examine the lists of clauses associated with these four fundamental principles and identify those which are most relevant:

- *2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.*

Somebody has misused the company's PC by using it to store images of child pornography. By this principle Joe has an obligation to report what he discovered.

- *2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.*
  While revealing the existence of the child pornography may harm the employee, possessing child pornography is illegal. Applying this principle would lead Joe to disclose what he discovered.
- *3.13. Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.*
  Joe discovered the child pornography by violating the company's policy against examining files on personal computers used by employees.
- *5.10. Provide for due process in hearing charges of violation of an employer's policy or of this Code.*
  Simply because Chuck had these files on his computer does not necessarily mean he is guilty. Perhaps someone else broke into Chuck's computer and stored the images there.

Our analysis is more complicated because Joe violated company policy to uncover the child pornography on Chuck's PC. Once he has this knowledge, however, the remaining principles guide Joe to reveal what he has discovered to the relevant authorities within the corporation, even though management may punish Joe for breaking the privacy policy. There is the possibility that Chuck is a victim. Someone else may be trying to frame Chuck or use his computer as a safe stash for their collection of images. Joe should be discreet until a complete investigation is completed and Chuck has had the opportunity to defend himself.

8.5.3 Anti-Worm

SCENARIO

The Internet is plagued by a new worm that infects PCs by exploiting a security hole in a popular operating system. Tim Smart creates an anti-worm that exploits the same security hole to spread from PC to PC. When Tim's anti-worm gets into a PC, it automatically downloads a software patch that plugs the security hole. In other words, it fixes the PC so that it is no longer vulnerable to attacks via that security hole [6].

Tim releases the anti-worm, taking precautions to ensure that it cannot be traced back to him. The anti-worm quickly spreads throughout the Internet, consuming large amounts of network bandwidth and entering millions of computers. To system administrators, it looks just like another worm, and they battle its spread the same way they fight all other worms [7].

Analysis

These fundamental principles are most relevant to the anti-worm scenario:

- Continually improve your abilities.
- Share your knowledge, expertise, and values.
- Respect the rights of others.
- Take responsibility for your actions and inactions.

Examining the list of clauses associated with each of these fundamental principles reveals those that are most relevant to our case study:

- *1.01. Accept full responsibility for their own work.*
  Tim tried to prevent others from discovering that he was the author of the anti-worm. He did not accept responsibility for what he had done.
- *1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.*
  The anti-worm did something good by patching security holes in PCs. Tim provided the anti-worm to the Internet community without charge. However, system administrators spent a lot of time trying to halt the spread of the anti-worm, a harmful effect.
- *2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or the employer's knowledge and consent.*
  Tim's "client" is the community of Internet PC owners who happen to use the operating system with the security hole. While his anti-worm was designed to benefit them, it entered their systems without their knowledge or consent. The anti-worm also consumed a great deal of network bandwidth without the consent of the relevant telecommunications companies.
- *8.01. Further their knowledge of developments in the analysis, specification, design, development, maintenance, and testing of software and related documents, together with the management of the development process.*
- *8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.*
- *8.06. Improve their knowledge of this Code, its interpretations, and its application to their work.*
  Tim followed the letter of these three clauses when he acquired a copy of the worm, figured out how it worked, and created a reliable anti-worm in a short period of time. The experience improved his knowledge and skills. Perhaps he should invest some time improving his ability to interpret and use the Code of Ethics!

According to some of these principles, Tim did the right thing. According to others, Tim was wrong to release the anti-worm. How do we resolve this dilemma? We can simplify our analysis by deciding that Tim's welfare is less

important than the public good. Using this logic, we will no longer consider the fact that Tim improved his technical knowledge and skills by developing and releasing the anti-worm.

That leaves us with three clauses remaining (1.01, 1.08, and 2.03). From the point of view of Clause 1.01, what Tim did was wrong. By attempting to hide his identity, Tim refused to accept responsibility for launching the anti-worm. He has clearly violated the Code of Ethics in this regard.

When we evaluate Tim's action from the point of view of Clause 1.08, we must determine whether his efforts were directed to a "good cause." Certainly Tim's anti-worm benefited the PCs it infected by removing a security vulnerability. However, it harmed the Internet by consuming large amounts of bandwidth, and it harmed system administrators, who spent time battling it. Because there were harmful as well as beneficial consequences, we cannot say that Tim's efforts were directed to a completely good cause.

Finally, let's evaluate Tim's action from the point of view of Clause 2.03. Even though the anti-worm was completely benevolent, Tim violated the property rights of the PC owners, because the anti-worm infected their PCs without authorization. Hence Tim's release of the anti-worm was wrong from the point of view of this Clause.

To summarize our analysis, Tim's release of the anti-worm is clearly wrong from the point of view of Clauses 1.01 and 2.03. It is also hard to argue that he satisfied the spirit of Clause 1.08. We conclude that Tim's action violated the Software Engineering Code of Ethics and Professional Practice. ~

8.6 Whistleblowing

All three case studies presented in the previous section involve the actions of a single individual. It is easy for us to assign moral responsibility to that person and to discuss how things might have turned out better if he or she had acted differently. Often, however, a product or decision is the cumulative result of the work of many people within a larger organization. Suppose somebody within the organization perceives a danger to the public but is unable to persuade the rest of the organization to make needed changes to eliminate that danger. Should that person go outside the organization with the information?

A **whistleblower** is someone who breaks ranks with an organization in order to make an unauthorized disclosure of information about a harmful situation after attempts to report the concerns through authorized organizational channels have been ignored or rebuffed [8]. Sometimes employees become whistleblowers out of fear that actions taken by their employer may harm the public; other times they have identified fraudulent use of tax dollars [9].

8.6.1 Morton Thiokol/NASA

On January 28, 1986, the space shuttle *Challenger* lifted off from Cape Canaveral. On board were seven astronauts, including schoolteacher Christa McAuliffe, the first civilian

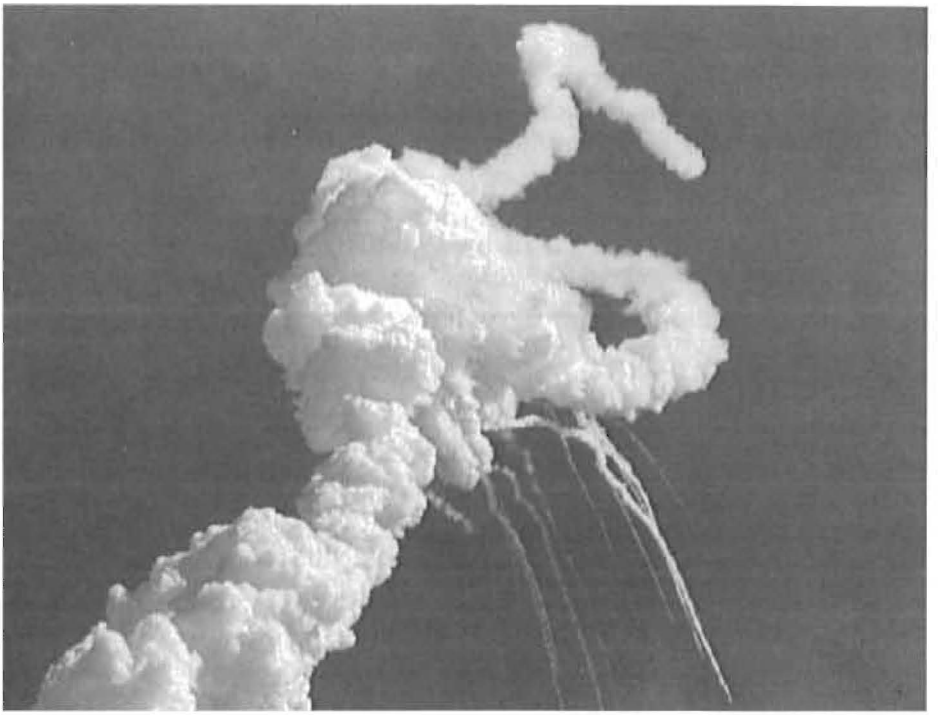

FIGURE 8.8 The explosion of the *Challenger* killed seven astronauts, including the first schoolteacher in space, Christa McAuliffe. (Courtesy of NASA)

to fly into space. Just 73 seconds after lift-off, hot gases leaking from one of the booster rockets led to an explosion that destroyed the *Challenger* and killed everyone on board (Figure 8.8).

Engineer Roger Boisjoly was in charge of inspecting the O-rings on the boosters recovered after launches of the space shuttle. The O-rings were supposed to seal connections between sections of the booster rockets. On two occasions in 1985 he had seen evidence that a primary O-ring seal had failed. Boisjoly presented a report on his findings to NASA officials at the Marshall Space Flight Center. Frustrated that NASA officials were not giving sufficient attention to the problem, he wrote a memo to Vice President for Engineering Robert Lund stating that an O-ring failure could lead to the loss of a shuttle flight and the launch pad. Despite Boisjoly's persistent efforts to get the seals redesigned, the problem was not fixed.

On January 27, 1986, Boisjoly and a group of Morton Thiokol engineers met to discuss the proposed launch for the following day. Florida was in the middle of an unusual cold snap; the weather forecast for northern Florida called for an overnight low of 18 degrees Fahrenheit. The engineers knew that frigid temperatures greatly increased the probability that an O-ring would fail, allowing hot gases to escape from a booster rocket. They prepared a set of 14 slides that documented their concern about a low-temperature launch.

The evening of January 27, Morton Thiokol had a teleconference with the Marshall Space Flight Center and the Kennedy Space Center. Morton Thiokol's presentation ended with the engineers' recommendation that NASA not launch the *Challenger* if the temperature was below 53 degrees. NASA asked Morton Thiokol Vice President Joe Kilminster for a go/no-go decision. Kilminster said his recommendation was not to launch.

NASA officials were displeased to get this recommendation from Morton Thiokol. The launch had already been delayed several times. They were eager to launch the space shuttle before the President's State of the Union address the following evening, so that the President could include the mission in his speech. After NASA officials expressed their dismay with the recommendation, Kilminster asked for a five-minute break in the proceedings.

During the recess, Morton Thiokol's four top managers huddled away from the engineers. Senior Vice President Jerald Mason and Vice President Calvin Wiggins supported the launch, while Vice Presidents Joseph Kilminster and Robert Lund were opposed. However, Lund changed his mind after Mason "told him to take off his engineering hat and put on his management hat" [10]. (More than half of Morton-Thiokol's profits came from its work for NASA.)

When Morton Thiokol rejoined the teleconference, Kilminster told NASA officials that Morton Thiokol recommended the launch go ahead. NASA officials at the Marshall Flight Center prevented the engineers' negative recommendation from being communicated to the NASA officials with final authority to approve or delay the launch.

A month after the loss of the *Challenger*, Boisjoly testified before a Presidential commission appointed to investigate the disaster. Morton Thiokol lawyers had advised Boisjoly to reply to every question with a simple "yes" or "no." Instead, Boisjoly shared with the commission his hypothesis about how the cold temperature had caused the failure of an O-ring. In later meetings with commission members, he presented documents that supported his hypothesis, including his 1985 memo. Boisjoly's testimony and documents contradicted the testimony of Morton Thiokol management. The company responded by isolating Boisjoly from NASA personnel and the O-ring redesign effort [10, 11].

Distressed by the hostile environment, Boisjoly stopped working for Morton Thiokol in July 1986. Two years later, he found work as a forensic engineer.

8.6.2 Hughes Aircraft

In the 1980s Hughes Aircraft manufactured military-grade hybrid computer chips at its Micro-electronic Circuit Division in Newport Beach, California. (A *hybrid computer chip* contains both digital and analog circuits.) The division produced about 100,000 hybrid chips per year. The military put these chips in a variety of sophisticated weapons systems, such as fighter planes and air-to-air missiles. Manufacturing these chips was a lucrative business for Hughes Aircraft; the government paid between $300 and $5,000 for each chip.

In return for paying these high prices, the government insisted that the chips pass stringent quality assurance tests. Hughes Aircraft technicians made two kinds of tests. First, they ensured the chips functioned correctly. Second, they checked the chips for resistance to shocks, high temperatures, and moisture. About 10 percent of the chips failed at least one of these tests. A common problem was that a chip would have a defective seal, which let moisture in. These chips were called "leakers."

Margaret Goodearl and Donald LaRue supervised the testing area. The company hired Ruth Ibarra to be an independent quality control agent.

In August 1986 floor worker Lisa Lightner found a leaker. Donald LaRue ordered her to pass the chip. Lightner told Goodearl, and Goodearl reported the incident to upper management. Hughes Aircraft management threatened to fire Goodearl if she didn't reveal the identity of the worker who had complained.

Two months later, LaRue ordered Shirley Reddick, another floor worker, to reseal lids on some hybrid chips, in violation of the required process for handling leakers. Reddick reported the incident to Goodearl, who relayed the report to upper management. Again, Goodearl was told she might be fired if she kept up this pattern of behavior.

In the same month, LaRue asked tester Rachel Janesch to certify that a defective hybrid chip had passed the leak test. Goodearl played a role in reporting the incident to Hughes Aircraft management. In this case, the chips were retested.

Goodearl and Ibarra found a box of hybrid chips with blank paperwork, meaning the necessary tests had not been performed. When Goodearl reported this discovery to her superiors, they told her she was no longer part of the team. Goodearl filed a formal harassment complaint. A mid-level manager in Personnel called her into his office, tore up her complaint, threw his glasses at her, and said, "If you ever do anything like that again, I will fire your ass" [9].

Goodearl's performance evaluations, which had been excellent, dropped sharply as soon as she began complaining about irregularities in the chip testing facility. In late 1986 Goodearl and Ibarra contacted the Office of the Inspector General, part of the U.S. Department of Justice. A joint decision was made for Goodearl and Ibarra to find a clear-cut case of fraud.

One day LaRue put two leaky hybrid chips on his desk, planning to approve them after Goodearl had gone home. Goodearl and Ibarra made photocopies of the documentation showing the chips had failed the leak test. After the chips were shipped from Hughes Aircraft, the Department of Defense tested them and found them to be leakers. As a result of this incident, the Office of the Inspector General began a formal investigation of fraud at Hughes Aircraft.

Hughes Aircraft fired Goodearl in 1989. Ibarra had left Hughes Aircraft in 1988, "after being relieved of all meaningful responsibilities and put in a cubicle with nothing to do" [12]. In 1990, Goodearl and Ruth Ibarra (now known under her married name, Ruth Aldred) filed a civil suit against Hughes Aircraft, claiming that Hughes Aircraft had violated the False Claims Act by falsifying records in order to defraud the government. This civil suit was put on hold until the end of the criminal trial.

The Inspector General's criminal investigation led to a trial in 1992. The jury found Hughes Aircraft guilty of conspiring to defraud the government. Hughes Aircraft appealed the verdict, but the verdict was upheld. Since a criminal conviction can be used as evidence in a civil trial, the verdict nearly assured that Goodearl and Alred would prevail in their civil suit. Hughes Aircraft began negotiating a settlement in the civil suit.

Four years later, Hughes Aircraft was ordered to pay $4.05 million in damages. Goodearl and Aldred received 22 percent of the settlement, or $891,000. In addition, Hughes Aircraft was required to pay their legal fees, which amounted to $450,000 [9, 13].

Goodearl and Aldred paid a high price for whistleblowing. Both were unemployed for an extended period of time. Aldred and her husband went on welfare until they could find work. Goodearl and her husband had to file for bankruptcy, and they eventually divorced. Despite these hardships, both whistleblowers said they "would do it all again" [14].

8.6.3 U.S. Legislation Related to Whistleblowing

Whistleblowers are usually punished for disclosing information that organizations have tried to keep under wraps. If they do not lose their job outright, they have probably lost all chances for future advancement within the organization. Whistleblowers and their families typically suffer emotional distress and economic hardship.

Nevertheless, whistleblowers often serve the public good. For this reason the U.S. government has passed two pieces of legislation to encourage whistleblowing: the False Claims Act and the Whistleblower Protection Act of 1989.

The False Claims Act was first enacted by Congress in 1863 in response to massive fraud perpetrated by companies providing supplies to the Union Army during the Civil War. The law allowed a whistleblower to sue, on behalf of the government, a person or company that was submitting falsified claims to the government. If the organization was found guilty and forced to pay a settlement to the government, the whistleblower received half of the settlement.

In 1943 Congress amended the False Claims Act, drastically reducing the share of the settlement a whistleblower would receive and limiting the evidence or information a whistleblower could use in the lawsuit. As a result, the law fell into disuse.

In the mid-1980s the media carried numerous stories about defense contractors perpetrating fraud against the government. Congress responded by amending the False Claims Act once again, making it easier for people to put together a successful lawsuit and allowing whistleblowers to receive between 15 and 30 percent of settlements. The False Claims Act also provides certain protections to whistleblowers against retaliation by their employers.

The Whistleblower Protection Act of 1989 establishes certain safeguards for federal employees and former employees who claim negative personnel actions have been taken against them for whistleblowing. Whistleblowers can appeal to the U.S. Merit Systems Protection Board.

8.6.4 Morality of Whistleblowing

Are whistleblowers heroes or traitors? Marcia Miceli and Janet Near point out that people become whistleblowers for different reasons. They suggest we ought to consider their motives before we decide if they were acting morally [15]. While it is fair to say that all whistleblowers are trying to bring an end to wrongdoing, they may well have other reasons for publicizing a problem. We can evaluate the morality of whistleblowing by considering whether the whistleblower is motivated by a desire to help others or harm others.

Consider a person who has known about a dangerous product for years, but only becomes a whistleblower after he has been turned down for a raise or promotion. If the disgruntled employee whistleblows in order to exact revenge on an organization that has let him down, the primary motivation is to hurt the company, not help the public.

Another example of questionable whistleblowing is the case of employees who have been involved in a cover-up for some period of time, realize that they are about to be caught, and then cooperate with the authorities to identify other guilty parties in order to avoid punishment.

But suppose a person doesn't have ulterior motives for whistleblowing and is doing it simply to inform the public of a dangerous situation or a misappropriation of funds. There are three general reactions to altruistic whistleblowing [11].

WHISTLEBLOWERS CAUSE HARM

The typical corporate response to whistleblowing is to condemn it. Whistleblowers are disloyal to their companies. Through their actions they generate bad publicity, disrupt the social fabric of an organization, and make it more difficult for everyone to work as part of a team. In other words, their betrayal causes short-term and long-term damage to the company. While it is the responsibility of engineers to point out technical problems, the management of a company is ultimately responsible for the decisions being made, both good and bad. If management makes a mistake, the public has recourse through the legal system to seek damages from the company, and the Board of Directors or CEO can replace the managers who have used bad judgment.

The weakness with this response is its cavalier and overly legalistic attitude toward public harm. If people are hurt or killed, they or their heirs can always sue for damages. Yet surely society is better off if people are not harmed in the first place. A monetary settlement is a poor replacement for a human life.

WHISTLEBLOWING IS A SIGN OF ORGANIZATIONAL FAILURE

A second response to whistleblowing is to view it as a symptom of an organizational failure that results in harm all around [16]. The company suffers from bad publicity. The careers of accused managers can be ruined. It makes people suspicious of one another, eroding team spirit. Whistleblowers typically suffer retaliation and become estranged from their coworkers. Labeled as troublemakers, their long-term prospects with the company are dim.

"I'm making this decision on principle, just to see how it feels."

Since whistleblowing is a sign of failure, organizations need to find a way to prevent it from happening in the first place. Some suggest that organizations can eliminate the need for whistleblowing by creating management structures and communication processes that allow concerns to be raised, discussed, and resolved.

This may be easier said than done. Robert Spitzer observes that organizations have shifted away from principle-based decision making to utilitarian decision making. A characteristic of rule-oriented ethical decision making is its absolute nature. According to Kantianism or social contract theory, the end never justifies the means. If an action violates a moral rule, it shouldn't be done, period. In contrast, a utilitarian process weighs expected benefits and harms. Once an organization begins using utilitarian thinking, the question is no longer, "Should we do it?" but, "How much of it can we do without harm?" Spitzer writes, "One can see situations in which it would be permissible to use an evil means to achieve a good so long as enough benefit can be actualized." He suggests that organizations should return to using principle-based ethics in their decision making [17].

WHISTLEBLOWING AS A MORAL DUTY

A third response is to assert that under certain circumstances people have a moral duty to whistleblow. Whistleblowing is alluded to in Clauses 1.02, 1.03, 1.04, 1.05, 2.05, 2.09, 3.01, 6.06, and 6.13 of the Software Engineering Code of Ethics and Professional

Practice. These clauses provide a justification for whistleblowing in a variety of circumstances.

Richard De George believes whistleblowers should ask themselves five questions:

1. Do you believe the problem may result in "serious and considerable harm to the public"?
2. Have you told your manager your concerns about the potential harm?
3. Have you tried every possible channel within the organization to resolve the problem?
4. Have you documented evidence that would persuade a neutral outsider that your view is correct?
5. Are you reasonably sure that if you do bring this matter to public attention, something can be done to prevent the anticipated harm?

According to De George, you have a right to whistleblow if you answer "yes" to the first three questions; if you answer "yes" to all five questions, you have a duty to whistleblow [18].

De George's five requirements are controversial. Some would say whistleblowing is justified even when fewer requirements are met. For example, what if the potential whistleblower knows about a problem that could result in the death or injury of millions of people, such as a meltdown inside a nuclear power plant? The whistleblower has communicated his concerns to his manager, but there is not time to lobby every potential decision maker in the company. He is reasonably sure that if he contacted a television station, something could be done to prevent the meltdown. At the very least the media could alert people so they could get out of harm's way. Shouldn't that person be obliged to whistleblow, even though the answer to the third question is "no"?

To others, insisting that the whistleblower have convincing documentation is too strict a condition to be met in order for whistleblowing to be a moral imperative. After all, once the whistleblower has revealed the wrong to another organization, that organization may be in a better position to gather supporting evidence than the whistleblower [19].

Along the same line, some argue that whistleblowing should be considered an obligation even when only the first three requirements are met. They hold that people should be willing to sacrifice their good and the good of their family for the greater good of society.

Others believe De George goes too far when he gives conditions under which people are morally *required* to whistleblow. These commentators suggest that a person's obligation to whistleblow must be weighed against that person's other obligations, such as the duty to take care of one's family. Whistleblowing often results in significant emotional stress and the loss of employment. If it results in a person being labeled a troublemaker, whistleblowing can end a career. Hence there are serious emotional and financial consequences to whistleblowing that affect not only whistleblowers but also their spouses and children [11].

Put another way, it is reasonable to take a strictly utilitarian approach to whistleblowing? Should we expect potential whistleblowers to weigh the benefits to a large number of people against the harm to themselves and their family, and decide to go public? After all, the whistleblower has already gone out on a limb to inform management of the dangerous situation. It is the managers who made the immoral decision to cover up the problem, not the whistleblower. We are asking a lot when we ask innocent people to sacrifice their career and the welfare of their family for the benefit of strangers. We shouldn't be surprised to learn that when whistleblower Al Ripskis was asked what advice he would give potential whistleblowers, his immediate reply was "Forget it!" [20].

On the other hand, whistleblower Carlos G. Bell, Jr., chastises fellow engineers for the way they duck responsibility:

> We engineers are almost without exception only too willing to assign moral responsibility to any administrator or executive or politician under whom we can place ourselves. Our reward for living in such ways is a part of the American dream: we are involved in very few arguments and year-by-year, we build up sizable pensions for our old age [21].

Moral responsibility is different from other kinds of responsibility. First of all, moral responsibility must be borne by people. While the Fourteenth Amendment to the Constitution may make a corporation a person in the legal sense of the word, a corporation is not a moral agent. We cannot assign moral responsibility to a corporation or any other organization [22].

Second, moral responsibility is different from role responsibility, causal responsibility, and legal responsibility in that it is not exclusive [22]. **Role responsibility** is responsibility borne because of a person's assigned duties. A company may hire a bookkeeper to send out invoices and pay the bills. It is the bookkeeper's responsibility to get the bills paid on time. **Causal responsibility** is responsibility assigned to people because they did something (or failed to do something) that caused something to happen. "Joe is responsible for the network being down, because he released the virus that caused the computers to crash." **Legal responsibility** is responsibility assigned by law. Homeowners are responsible for the medical bills of a postal carrier who slips and falls on their driveway. Role responsibility, causal responsibility, and legal responsibility can be exclusive. For example, if one person is responsible for paying the bills, the other employees are not. Moral responsibility is not exclusive. For example, if an infant is brought into a home, both the mother and the father are responsible for the baby's well-being.

Because moral responsibility is not exclusive, people cannot pass the buck by saying, "My boss made the final decision, not me," or by saying, "I just wrote the software; I wasn't responsible for testing it." When people abdicate their moral responsibility, great harms can be done. In the 1970s executives at Ford Motor Company were anxious to begin selling a 2,000 pound, $2,000 alternative to Japanese imports. Unfortunately, prototypes of the Ford Pinto could not pass the mandatory collision test, because the windshield kept popping out. Forbidden from making design changes that would increase the weight of the car or delay its introduction, engineers solved the problem by redirecting the energy of the collision down the drive train to the gas tank. They knew

this change would make the gas tank more likely to rupture, but the car did not have to pass a fuel tank integrity test. Covering up design problems allowed Ford to get its subcompact car to market. However, Ford eventually paid millions of dollars to settle dozens of lawsuits resulting from fiery crashes involving Pintos. Moreover, unfavorable media attention harmed Ford's reputation for years [20].

Michael McFarland argues that a team of engineers should be held to a higher level of moral responsibility than any of its individual members. There may well be situations where a person has a duty to speak the truth. To this duty, McFarland adds another duty held by moral agents: the duty to help others in need. If whistleblowing should be done, and no individual has the strength to do it, then it must be done by the group acting collectively [23].

Summary

A computer-related job, such as system administration, computer programming, or software engineering, is not a full-fledged profession like medicine or law, because you do not need to be certified and licensed in order to design, implement, or maintain computer hardware or software. Nevertheless, those who work with computers can, through inadequate education, insufficient practical training, or bad choices, cause a great deal of harm to members of the public. In this respect the responsibility of computer "professionals" can be similar to that held by members of fully developed professions. For these reasons the two largest computing societies have worked together to develop a code of ethics to guide the actions of software engineers: those who develop or maintain software, or teach in this area.

The Software Engineering Code of Ethics and Professional Practice is based upon eight general principles related to the following subjects: the public, client and employer, product, judgment, management, profession, colleagues, and self. Each of these general principles contains a list of clauses related to specific areas of potential moral concern for the practicing software engineer. Good judgment is still needed, however. In many situations there is a conflict between two or more of the relevant clauses. At these times the decision-maker must determine which of the clauses is most relevant and/or most important.

The Code of Ethics asks software engineers to ponder if their actions are worthy of the ideal professional. The ethics of virtue, or virtue ethics, is based on the imitation of morally superior role models. Virtue ethics arises from Aristotle's belief that happiness is the result of living a virtuous life. One of the strengths of virtue ethics is that it makes clear how good deeds are motivated by friendship, loyalty, dependability, and other praiseworthy attributes of a good person. Another strength of virtue ethics—at least according to its supporters—is that it does not demand that every action produce the maximum benefit, solving the problem of impartiality that plagues Kantianism, utilitarianism, and social contract theory. On the other hand, virtue ethics does not provide a formal process for moral decision making: using virtue ethics alone, it is not always clear what a person is supposed to do in a particular situation. For this reason

some philosophers argue that virtue ethics should be used as a complement to another theory, such as utilitarianism, rather than as a stand-alone ethical theory.

To many, whistleblowing is a heroic act requiring great moral courage. A whistleblower brings to light a real or potential harm to the public, such as an abuse of taxpayer's money or a defective product, after trying and failing to get the problem resolved within the organization. Inevitably, whistleblowers and their families suffer emotionally and economically. It may take a decade for a whistleblower to be vindicated in court.

Different commentators have taken widely different views about whistleblowing. Some say whistleblowing does so much harm to the whistleblower and the organization that it is never the right thing to do. At the other extreme are those who argue any harm done to whistleblowers and their families is outweighed by the benefits to society, at least when certain conditions are met. In the middle are those who argue that any decision for or against whistleblowing must be made on a case-by-case basis.

If whistleblowing is ever called for, it is only as a last resort. Everyone agrees that people who discover real or potential harms to the public should first attempt to get the problem fixed within the organization. It would be better if there were never a need for whistleblowing. Organizations ought to have communication and decision-making structures that make it easier to identify and deal with financial irregularities or product defects.

The predominant American corporate mindset does not align well with this ideal. Managers focused on maximizing "the bottom line" may well make decisions on utilitarian grounds, weighing the costs and benefits of each alternative. Utilitarian thinking allows an organization to do something that is slightly bad in order to reap a greater good. Undisclosed bad deeds are less harmful than those brought to the light. Hence utilitarian thinking can create an atmosphere in which the free communication of organizational actions is suppressed. In this environment, those who wish to report financial irregularities or product defects are ignored or silenced. The financial scandals at Enron, Tyco International, WorldCom, Adelphia Communications, and other corporations that cost investors billions of dollars have prompted some ethicists to call for a return to principle-based decision making.

Review Questions

1. What is a profession? How is a computer-related career, such as programming or system administration, similar to a fully developed profession, such as medicine? How is a computer-related career unlike a fully developed profession?
2. Why did the ACM pass a resolution opposed to the licensing of software engineers?
3. Identify as many clauses as you can in the Software Engineering Code of Ethics and Professional Practice that refer to issues related to privacy.
4. Identify as many clauses as you can in the Software Engineering Code of Ethics and Professional Practice that refer to issues related to intellectual property.

5. Identify five clauses in the Software Engineering Code of Ethics and Professional Practice that reflect a utilitarian ethical viewpoint.
6. Identify five clauses in the Software Engineering Code of Ethics and Professional Practice that reflect a Kantian viewpoint.
7. Describe virtue ethics in your own words.
8. What are the advantages and disadvantages of virtue ethics?
9. The text gives James Rachels's short list of 24 virtues. Come up with a list of 5 additional virtues.
10. What is whistleblowing? What harms does it cause? What benefits may it provide?
11. Which clauses in the Software Engineering Code of Ethics and Professional Practice support the legitimacy of whistleblowing? Which clauses in the Code may be violated by a whistleblower (assuming the whistleblower is telling the truth)?

Discussion Questions

12. The *Challenger* disaster led to the deaths of seven astronauts and the loss of hundreds of millions of dollars worth of equipment. How much moral responsibility should each of the following groups hold for this tragedy: Morton-Thiokol engineers, Morton-Thiokol senior management, NASA management?
13. In the criminal proceedings resulting from the government's investigation of fraud at the Micro-electronic Circuit Division, the jury found Hughes Aircraft guilty, but it found supervisor Donald LaRue not guilty. The jury felt LaRue was simply following orders from management. Was the jury's decision a just one?
14. Do you agree with Michael McFarland that a team of engineers has greater moral responsibility than any individual engineer on the team?
15. You are a manager in charge of a section of 30 employees in a large corporation. This morning one of your employees—Jane Lee—enters your office and tells you she thinks two members of your staff are having an affair. These employees are married—but not to each other. Jane is afraid that if it is true, others in the office will inevitably find out about it, harming morale and productivity. She suggest that you discreetly monitor their emails to see if it provides evidence of an affair. If you find evidence, you can nip the problem in the bud. If there is no problem, you do not have to embarrass yourself by talking with the employees. What should you do? [24]
16. According to virtue ethics, the right action to take in a particular situation is the action that a person with strong moral character would take. If you decide to practice virtue ethics, you need to find a moral role model. How would you choose a role model?
17. Two weeks ago you started a new job as system administrator for a computer lab at a small college. Wanting to make a good impression, you immediately set out to learn more about the various applications provided to the users of the lab. One of the packages, an engineering design tool, seemed way out of date. You looked through the lab's file of licensing agreements to see how much it would cost to get an upgrade. To your

horror, you discovered that the college never purchased a license for the software—it is running a bootlegged copy!

When you bring this to the attention of your boss, the college's Director of Information Technology, he says, "The license for this software would cost us $10,000, which we don't have in our budget right now. This software is absolutely needed for our engineering students, though. Maybe we can get the license next year. For the time being, just keep the current version running."

How would you respond to your manager?

18. You are a junior in college. You sent your resume to a half-dozen companies hoping to get a summer internship. Two weeks ago XYZ Corporation contacted you and offered you a paid summer internship. One week ago you accepted their offer, agreeing to start work a week after your last final exam. Today you received a much better internship offer from ABC Corporation. What should you do?

19. You are a senior in college. You sent your resume to a half-dozen companies hoping to get a job. A month ago you interviewed at ABC Corporation and XYZ Corporation. Two weeks ago XYZ Corporation offered you a job. One week ago you accepted their offer, agreeing to start work a month after graduation. Today you received a much better offer from ABC Corporation. What should you do?

20. You are the manager of a software development group within a large corporation. Your group would be more productive if the PCs were upgraded, but you do not have any money left in your annual equipment budget. Because of employee turnover, you do have plenty of money left in your personnel budget, but corporate rules do not allow you to spend personnel funds on equipment.

    If you overspend your equipment budget, you will receive a negative performance review. You also know that whatever money is left over in your budget at the end of the fiscal year is "swept up" by the corporation. In other words, you cannot carry over a surplus from one year to the next—your group loses the money.

    You complain about your situation to the manager of another group, who has the opposite problem. She has plenty of money left in her equipment budget, but her personnel expenses are going to exceed her labor budget unless she does something. She offers to buy you the $50,000 of equipment you need out of her budget, if you pick up $50,000 of her personnel expenses out of your budget. If you take this action, both groups will get what they need, and neither group will exceed any of its budgets.

    Discuss the morality of the proposed course of action.

In-class Exercises

21. A college equips its large lecture halls with wireless networks, and it requires all of its students to purchase a laptop computer when they enroll. A computer science professor plans to streamline how quizzes are administered in his introductory programming class. Students will take the quizzes online as they sit in the classroom. A computer will grade the quizzes instantly, providing the students with instant feedback. The computer will also provide the professor with information about how well the students did on each

question, which will enable him to spend more of his lecture time focusing on those topics that the students are having the hardest time understanding. Discuss the benefits and risks associated with implementing the proposed system.

22. Company X wants to open a dating service Web site. It hires Company Y to develop the software. Company Y hires Gina as a private contractor to provide a piece of instant messaging software for the package. Gina's contract says she is not responsible for the security of the site. Company Y is supposed to perform that bit of programming. However, software development runs behind schedule, and Company Y implements a simplistic security scheme that allows all messages to be sent in plain text, which is clearly insecure.

    Gina brings her concerns to the management of Company Y. Company Y thanks her for her concern, but indicates it still plans to deliver the software without telling Company X. Company Y reminds Gina that she has signed a confidentiality agreement that forbids her from talking about the software to anyone, including Company X.

    What should Gina do?

23. You are members of the information services team at a large corporation. The President has asked for a confidential meeting with your group to talk about ways to improve productivity. The President wants to ensure that people are not sending personal emails or surfing the Web for entertainment while they are supposed to be working. The Chief Information Officer suggests that employees be informed that their emails and Web surfing will be monitored. In truth, the company does not have the resources to do this and does not plan to implement any monitoring. The CIO strictly forbids anyone in the information services team from revealing this fact. Debate the morality of management making such an announcement.

24. The members of the class are the employees of a small, privately held company that produces computer games. Everyone shares in the profits of the company. The company has been making electronic versions of popular board games for established game companies. Business is steady, but profits have not been large. The marketing team says that a first-person shooter game based on the war in Iraq would generate a huge amount of publicity for the company and could be highly profitable. Debate the morality of producing such a game.

Further Reading

Association for Computing Machinery Web site. www.acm.org.

Margaret Coady and Sidney Bloch, editors. *Codes of Ethics and the Professions*. Melbourne University Press, Melbourne, Australia, 1996.

ComputingCases.org (Web site).

Myron Peretz Glazer and Penina Migdal Glazer. *The Whistleblowers: Exposing Corruption in Government and Industry*. Basic Books, New York, NY, 1989.

IEEE Computer Society Web site. www.computer.org.

Deborah G. Johnson. *Ethical Issues in Engineering*. Prentice Hall, Englewood Cliffs, NJ, 1991.

Alasdair MacIntyre. *After Virtue*. 2nd ed. University of Notre Dame Press, Notre Dame, IN, 1984.

Mike W. Martin. *Meaningful Work: Rethinking Professional Ethics*. Oxford University Press, New York, NY, 2000.

Justin Oakley and Dean Cocking. *Virtue Ethics and Professional Roles*. Cambridge University Press, Cambridge, England, 2001.

References

[1] Gary Ford and Norman E. Gibbs. "A Mature Profession of Software Engineering." Technical report, Carnegie-Mellon University, January 1996. CMU/ SEI-96-TR-004, ESC-TR-96-004.

[2] Fran Allen (co chair), Barry Boehm, Fred Brooks, Jim Browne, Dave Farber, Sue Graham, Jim Gray, Paula Hawthorn (co chair), Ken Kennedy, Nancy Leveson, Dave Nagel, Peter Neumann, Dave Parnas, and Bill Wulf. "ACM Panel and Professional Licensing in Software Engineering Report to Council." May 15, 1999. www.acm.org/serving/se_policy.

[3] Aristotle. *The Nicomachean Ethics*. Oxford University Press, Oxford, England, 1998. Translated by F. H. Peters and M. Ostwald.

[4] James Rachels. *The Elements of Moral Philosophy*. 4th ed. McGraw-Hill, Boston, MA, 2003.

[5] Justin Oakley and Dean Cocking. *Virtue Ethics and Professional Roles*. Cambridge University Press, Cambridge, England, 2001.

[6] J. Eric Smith. "Anti-worm Worm Makes Rounds, Cleanses Systems of Infection." *GEEK.com*, August 20, 2003.

[7] Florence Olsen. "Attacks Threaten Computer Networks as Students Arrive for the Fall Semester." *The Chronicle of Higher Education*, September 5, 2003.

[8] Irena Blonder. "Blowing the Whistle." In *Codes of Ethics and the Professions*, pages 166–190. Melbourne University Press, Melbourne, Australia, 1996.

[9] Kevin W. Bowyer. "Goodearl and Aldred versus Hughes Aircraft: A Whistle-Blowing Case Study." In *Frontiers in Education*, pages S2F2–S2F7. October 2000.

[10] Roger M. Boisjoly. "The Challenger Disaster: Moral Responsibility and the Working Engineer." In *Ethical Issues in Engineering*, pages 6–14. Edited by Deborah G. Johnson. Prentice Hall, Englewood Cliffs, NJ, 1991.

[11] Mike W. Martin. *Meaningful Work: Rethinking Professional Ethics*. Oxford University Press, New York, NY, 2000.

[12] Taxpayers Against Fraud. *U.S. Department of Justice Joins Whistle-blowers in Lawsuit Against Hughes Aircraft Seeking Several Hundred Million Dollars*. December 15, 1992. Press release.

[13] "The Hughes Whistleblowing Case." *ComputingCases.org*.

[14] Andre Mouchard. "Whistle-Blowers Set to Use Their Reward." *The Orange County Register (California)*, September 11, 1996.

[15] Marcia P. Miceli and Janet P. Near. "Whistle-Blowing as Antisocial Behavior." In *Antisocial Behavior in Organizations*. SAGE Publications, Thousand Oaks, CA, 1997.

[16] Michael Davis. "Avoiding the Tragedy of Whistleblowing." *Business and Professional Ethics Journal*, 8(4):3–19, Winter 1989.

[17] Robert J. Spitzer, S.J. "For Good Reason, 'Organizational Ethics' a Hot Topic Nowadays." *Gonzaga (Gonzaga University newsletter)*, 5(2):2, Fall 2003.

[18] Richard T. DeGeorge. *Business Ethics*. 3rd ed. Macmillan, New York, NY, 1990.

[19] Gene G. James. "Whistle Blowing: Its Moral Justification." In *Business Ethics*, 2nd ed., pages 332–344. McGraw-Hill, New York, NY, 1990.

[20] Myron Peretz Glazer and Penina Migdal Glazer. *The Whistleblowers: Exposing Corruption in Government and Industry*. Basic Books, New York, NY, 1989.

[21] Bell, Carlos G., Jr. "One Ethical Problem Faced by the Atomic Energy Commission and Its Contractors." In *Beyond Whistleblowing: Defining Engineers' Responsibilities, Proceedings of the Second National Conference on Ethics in Engineering*, pages 250–258. Illinois Institute of Technology, Chicago, IL, 1983.

[22] John Ladd. "Collective and Individual Moral Responsibility in Engineering: Some Questions." In *Beyond Whistleblowing: Defining Engineers' Responsibilities, Proceedings of the Second National Conference on Ethics in Engineering*, pages 90–113. Illinois Institute of Technology, Chicago, IL, 1983.

[23] Michael McFarland. "The Public Health, Safety, and Welfare: An Analysis of the Social Responsibility of Engineers." In *Ethical Issues in Engineering*, edited by D. G. Johnson, pages 159–174. Prentice Hall, Englewood Cliffs, NJ, 1991.

[24] Herbert W. Lovelace. "When Affairs of the Heart Raise IT Privacy Issues." *InformationWeek.com*, December 10, 2001.