

9

PROFESSIONAL ETHICS AND RESPONSIBILITIES

9.1 WHAT IS PROFESSIONAL
ETHICS?

9.2 ETHICAL GUIDELINES
FOR COMPUTER PROFESSIONALS

9.3 SCENARIOS

EXERCISES



9.1 What Is Professional Ethics?

The scope of the term “computer ethics” varies considerably. It can include such social and political issues as the impact of computers on employment, the environmental impact of computers, whether or not to sell computers to totalitarian governments, use of computers by the military, and the consequences of the technological and thus economic divisions between developed countries and poor countries. It can include personal dilemmas about what to post on the Internet and what to download. In this chapter we focus more narrowly on a category of professional ethics, similar to medical, legal, and accounting ethics, for example. We consider ethical issues a person might encounter as a computer professional, on the job. Professional ethics includes relationships with and responsibilities toward customers, clients, coworkers, employees, employers, others who use one’s products and services, and others whom they affect. We examine ethical dilemmas and guidelines related to actions and decisions of individuals who create and use computer systems. We look at situations where you must make critical decisions, situations where significant consequences for you and others could result.

Extreme examples of lapses in ethics in many fields regularly appear in the news. In business, we had Enron, for example. In journalism, we have had numerous incidents of journalists at prominent news organizations plagiarizing or inventing stories. In science, a famed and respected researcher published falsified stem cell research and claimed accomplishments he had not achieved. A writer invented dramatic events in what he promoted as a factual memoir of his experiences. These examples involve blatant dishonesty, which is almost always wrong.

Honesty is one of the most fundamental ethical values. We all make hundreds of decisions all day long. The consequences of some decisions are minor. Others are huge and affect people we never meet. We base decisions, partly, on the information we have. (It takes ten minutes to drive to work. This software has serious security vulnerabilities. What you post on a social-network site is available only to your designated friends.) We pick up bits and pieces of information from explicit research, from conversations, and from our surroundings and regular activities. Of course, not all of it is accurate. But we must base our choices and actions on what we know. A lie deliberately sabotages this essential activity of being human: absorbing and processing information and making choices to pursue our goals. Lies are often attempts to manipulate people. As Kant would say, a lie treats people as merely means to ends, not ends in themselves. Lies can have many negative consequences. In some circumstances, lying casts doubt on the work or word of other people unjustly. Thus it hurts those people, and it adds unnecessary uncertainty to decisions by others who would have acted on the word of people the lie contradicts. Falsifying research or other forms of work is an indirect form of theft of research funds and salary. It wastes resources that others could have used productively. It contributes to incorrect choices and decisions by people who depend on the results of the work. The costs and indirect effects of lies can cascade and do much harm.

Many ethical problems are more subtle than the choice of being honest or dishonest. In health care, for example, doctors and researchers must decide how to set priorities for organ transplant recipients. Responsible computer professionals confront issues such as, How much risk (to privacy, security, safety) is acceptable in a system? What uses of another company's intellectual property are acceptable?

Suppose a private company asks your software company to develop a database of information obtained from government records, perhaps to generate lists of convicted shoplifters or child molesters or marketing lists of new home buyers, affluent boat owners, or divorced parents with young children. The people who will be on the lists did not have a choice about whether the information would be open to the public. They did not give permission for its use. How will you decide whether to accept the contract? You could accept on the grounds that the records are already public and available to anyone. You could refuse in opposition to secondary uses of information that people did not provide voluntarily. You could try to determine whether the benefits of the lists outweigh the privacy invasions or inconveniences they might cause for some people. You could refuse to make marketing lists, but agree to make lists of people convicted of certain crimes, using Posner's principle that negative information, such as convictions, should be in the public domain (see Section 2.4.2). The critical first step, however, is recognizing that you face an ethical issue.

The decision to distribute software to convert files from formats with built-in copy protection to formats that can be copied more easily has an ethical component. So too does the decision about how much money and effort to allocate to training employees in the use of a new computer system. We have seen that many of the related social and legal issues are controversial. Some ethical issues are also.

There are special aspects to making ethical decisions in a professional context, but the decisions are based on general ethical principles and theories. Section 1.4 describes these general principles. It would be good to reread or review it now. In Section 9.2 we consider ethical guidelines for computer professionals. In Section 9.3, we consider sample scenarios.

9.2 Ethical Guidelines for Computer Professionals

9.2.1 SPECIAL ASPECTS OF PROFESSIONAL ETHICS

Professional ethics have several characteristics different from general ethics. The role of the professional is special in several ways. First, the professional is an expert in a field, be it computer science or medicine, that most customers know little about. Most of the people affected by the devices, systems, and services of professionals do not understand how they work and cannot easily judge their quality and safety. This creates special responsibilities for the professional. Customers rely on the knowledge, expertise, and honesty of the professional. A professional advertises his or her expertise and thus has an obligation to provide it. Second, the products of many professionals (e.g., highway

bridges, investment advice, surgery protocols, and computer systems) profoundly affect large numbers of people. A computer professional's work can affect the life, health, finances, freedom, and future of a client or members of the public. A professional can cause great harm through dishonesty, carelessness, or incompetence. Often the victims have little ability to protect themselves. The victims, often, are not the direct customers of the professional and have no direct control or decision-making role in choosing the product or making decisions about its quality and safety. Thus, computer professionals have special responsibilities not only to their customers, but also to the general public, to the users of their products, regardless of whether they have a direct relationship with the users. These responsibilities include thinking about potential risks to privacy and security of data, safety, reliability, and ease of use. They include taking action to diminish risks that are too high.

In Chapter 8, we saw some of the minor and major consequences of flaws in computer systems. In some of those cases, people acted in clearly unethical or irresponsible ways. In many cases, however, there was no ill intent. Software can be enormously complex, and the process of developing it involves communications between many people with diverse roles and skills. Because of the complexity, risks, and impact of computer systems, a professional has an ethical responsibility not simply to avoid intentional evil, but to exercise a high degree of care and follow good professional practices to reduce the likelihood of problems. That includes a responsibility to maintain an expected level of competence and be up-to-date on current knowledge, technology, and standards of the profession. Professional responsibility includes knowing or learning enough about the application field to do a good job. Responsibility for a noncomputer professional using a sophisticated computer system includes knowing or learning enough about the system to understand potential problems.

In Section 1.4.1, we observed that although courage is often associated with heroic acts, we have many opportunities to display courage in day-to-day life by making good decisions that might be unpopular. Courage in a professional setting could mean admitting to a customer that your program is faulty, declining a job for which you are not qualified, or speaking out when you see someone else doing something wrong.

9.2.2 PROFESSIONAL CODES OF ETHICS

Many professional organizations have codes of professional conduct. They provide a general statement of ethical values and remind people in the profession that ethical behavior is an essential part of their job. The codes provide reminders about specific professional responsibilities. They provide valuable guidance for new or young members of the profession who want to behave ethically but do not know what is expected of them, people whose limited experience has not prepared them to be alert to difficult ethical situations and to handle them appropriately.

There are several organizations for the range of professions included in the general term *computer professional*. The main ones are the ACM and the IEEE Computer Society

(IEEE CS).¹ They developed the Software Engineering Code of Ethics and Professional Practice (adopted jointly by the ACM and IEEE CS) and the ACM Code of Ethics and Professional Conduct (both in Appendix A). We refer to sections of the Codes in the following discussion and in Section 9.3, using the shortened names SE Code and ACM Code. The Codes emphasize the basic ethical values of honesty and fairness.* They cover many aspects of professional behavior, including the responsibility to respect confidentiality,[†] maintain professional competence,[‡] be aware of relevant laws,[§] and honor contracts and agreements.[¶] In addition, the Codes put special emphasis on areas that are particularly (but not uniquely) vulnerable from computer systems. They stress the responsibility to respect and protect privacy,^{||} avoid harm to others,** and respect property rights (with intellectual property and computer systems themselves as the most relevant examples).^{††} The SE Code covers many specific points about software development. It is translated into several languages, and various organizations have adopted it as their internal professional standard.

Managers have special responsibility because they oversee projects and set the ethical standards for employees. Principle 5 of the SE Code includes many specific guidelines for managers.

9.2.3 GUIDELINES AND PROFESSIONAL RESPONSIBILITIES

We highlight a few principles for producing good systems. Most concern software developers, programmers, and consultants. A few are for professionals in other areas who make decisions about acquiring computer systems for large organizations. Many more specific guidelines appear in the SE Code and in the ACM Code, and we introduce and explain more in the scenarios in Section 9.3.

Understand what success means. After the utter foul-up on opening day at Kuala Lumpur's airport, blamed on clerks typing incorrect commands, an airport official said, "There's nothing wrong with the system." His statement is false, and the attitude behind the statement contributes to the development of systems that will fail. The official defined the role of the airport system narrowly: to do certain data manipulation correctly, assuming all input is correct. Its true role was to get passengers, crews, planes, luggage, and cargo to the correct gates on schedule. It did not succeed. Developers and institutional users of computer systems must view the system's role and their responsibility in a wide enough context.

*SE Code: 1.06, 2.01, 6.07, 7.05, 7.04; ACM Code: 1.3, 1.4

†SE Code: 2.05; ACM Code: 1.8

‡SE Code: 8.01–8.05; ACM Code: 2.2

§SE Code: 8.05; ACM Code: 2.3

¶ACM Code: 2.6

||SE Code: 1.03, 3.12; ACM Code: 1.7

**SE Code: 1.03; ACM Code: 1.2

††SE Code: 2.02, 2.03; ACM Code: 1.5, 1.6, 2.8

Include users (such as medical staff, technicians, pilots, office workers) in the design and testing stages to provide safe and useful systems. Recall the discussion of computer controls for airplanes (Sections 8.1.4 and 8.3.2), where confusing user interfaces and system behavior increased the risk of accidents. There are numerous “horror stories” in which technical people developed systems without sufficient knowledge of what was important to users. For example, a system for a newborn nursery at a hospital rounded each baby’s weight to the nearest pound. For premature babies, the difference of a few ounces is crucial information.² The responsibility of developers to talk to users is not limited to systems that affect safety and health. Systems designed to manage stories for a news Web site, to manage inventory in a toy store, or to organize documents and video on a Web site could cause frustration, waste a client’s money, and end up in the trash heap if designed without sufficient consideration of the needs of actual users.

The box on the next page illustrates more ways to think about your users.

Do a thorough, careful job when planning and scheduling a project and when writing bids or contracts. This includes, among many other things, allocating sufficient time and budget for testing and other important steps in the development process. Inadequate planning is likely to lead to pressure to cut corners later. (See SE Code 3.02, 3.09, and 3.10.)

Design for real users. We have seen several cases where computers crashed because someone typed input incorrectly. In one case, an entire pager system shut down because a technician did not press the Enter key (or did not hit it hard enough). Real people make typos, get confused, or are new at their job. It is the responsibility of the system designers and programmers to provide clear user interfaces and include appropriate checking of input. It is impossible for computers to detect all incorrect input, but there are techniques for catching many kinds of errors and for reducing the damage that errors cause.

Don’t assume existing software is safe or correct. If you use software from another application, verify its suitability for the current project. If the software was designed for an application where the degree of harm from a failure was small, the quality and testing standards might not have been as high as necessary in the new application. The software might have confusing user interfaces that were tolerable (though not admirable) in the original application but could have serious negative consequences in the new application. We saw in Chapter 8 that a complete safety evaluation is important even for software from an earlier version of the same application if a failure would have serious consequences. (Recall the Therac-25 and Ariane 5.)

Be open and honest about capabilities, safety, and limitations of software. In several cases described in Chapter 8, there is a strong argument that the treatment of customers was dishonest. Honesty of salespeople is hardly a new issue. The line between emphasizing your best qualities and being dishonest is not always clear, but it should be clear that hiding known, serious flaws and lying to customers are on the wrong side of the line.

Honesty includes taking responsibility for damaging or injuring others. If you break a neighbor’s window playing ball or smash into someone’s car, you have an obligation to pay for the damage. If a business finds that its product caused injury, it should not hide that fact or attempt to put the blame on others.

REINFORCING EXCLUSION

A speaker-recognition system is a system (consisting of hardware and software) that identifies the person speaking. (This is different from speech recognition, discussed in Section 7.5.2, which identifies the words spoken.) One application of speaker recognition is teleconferencing for business meetings. The computer system identifies who is speaking and displays that person on everyone's screens. Some speaker-recognition systems recognize male voices much more easily than female voices. Sometimes when the system fails to recognize female speakers and focus attention on them, they are effectively cut out of the discussion.³ Did the designers of the system intentionally discriminate against women? Probably not. Are women's voices inherently more difficult to recognize? Probably not. What happened? There are many more male programmers than female programmers. There are many more men than women in high-level business meetings. Men were the primary developers and testers of the systems. The algorithms were optimized for the lower range of male voices.

In his book *The Road Ahead*, Bill Gates tells us that a team of Microsoft programmers developed and tested a handwriting recognition system. When they thought it was working fine, they brought it to him to try. It failed. All the team members were right-handed. Gates is left-handed.⁴

In some applications, it might make sense to focus on a niche audience or ignore a special audience, but that choice should be conscious (and reasonable). These examples show how easy it is to develop systems that unintentionally exclude people—and how important it is to think beyond one's own group when designing and testing a system. Besides women and left-handed people, other groups to consider are nontechnical users, different ethnic groups, disabled people, older people (who might, for example, need a large-font option), and children.

In these examples, doing “good” or “right” in a social sense—taking care not to reinforce exclusion of specific groups of people—coincides with producing a good product and expanding its potential market.

Honesty about system limitations is especially important for *expert systems*, or decision systems, that is, systems that use models and heuristics incorporating expert knowledge to guide decision making (for example, medical diagnoses or investment planning). Developers must explain the limitations and uncertainties to users (doctors, financial advisors, and so forth, and to the public when appropriate). Users must not shirk responsibility for understanding them and using the systems properly.

Require a convincing case for safety. One of the most difficult ethical problems that arises in safety-critical applications is deciding how much risk is acceptable. Burning gases that leaked from a rocket shortly after launch destroyed the space shuttle Challenger, killing

the seven people aboard. A comment from one of the engineers who opposed the launch sheds some light on how subtle shifts in attitude can affect a decision. The night before the scheduled launch, the engineers argued for a delay. They knew the cold weather posed a severe threat to the shuttle. We cannot prove absolutely that a system is safe, nor can we usually prove absolutely that it will fail and kill someone. The engineer reported that, in the case of the Challenger, “It was up to us to prove beyond a shadow of a doubt that it was not safe to [launch].” This, he said, was the total reverse of a usual Flight Readiness Review.⁵ For the ethical decision maker, the policy should be to suspend or delay use of the system in the absence of a convincing case for safety, rather than to proceed in the absence of a convincing case for disaster.

Pay attention to defaults. Everything, it seems, is customizable: the level of encryption on a cell phone or wireless network, whether consumers who buy something at a Web site will go on an e-mail list for ads, the difficulty level of a computer game, the type of news stories your favorite news site displays for you, what a spam filter will filter out. So the default settings might not seem important. They are. Many people do not know about the options they can control. They do not understand issues of security. They often do not take the time to change settings. System designers should give serious thought to default settings. Sometimes protection (of privacy or from hackers, for example) is the ethical priority. Sometimes ease of use and compatibility with user expectations is a priority. Sometimes priorities conflict.

Develop communications skills. A computer security consultant told me that often when he talks to a client about security risks and the products available to protect against them, he sees the client’s eyes glaze over. It is a tricky ethical and professional dilemma for him to decide just how much to say so that the client will actually hear and absorb it.

There are many situations in which a computer professional has to explain technical issues to customers and coworkers. Learning how to organize information, distinguishing what is important to communicate and what is not, engaging the listener actively in the conversation to maintain interest, and so on, will help make one’s presentations more effective and help to ensure that the client is truly informed.

9.3 Scenarios

9.3.1 INTRODUCTION AND METHODOLOGY

The cases we present here, some based on real incidents, are just a few samples of the kinds that occur. They vary in seriousness and difficulty, and they include situations that illustrate professional responsibilities to potential users of computer systems in the general public, customers or clients, the employer, coworkers, and others. More scenarios appear in the exercises at the end of the chapter.

In most of this book, I have tried to give arguments on both sides of controversial issues without taking a position. Ethical issues are often even more difficult than some of the others we have covered, and there could well be disagreement among computer-ethics

specialists on some points in the cases considered here. In any real case, there are many other relevant facts and details that affect the conclusion. In spite of the difficulty of drawing ethical conclusions, especially for brief scenarios, for some of these cases I give conclusions. You might face cases like these where you have to make a decision. I do not want to leave the impression that, because a decision is difficult or because some people benefit or lose either way, there is no ethical basis for making the decision. (It seems ethically irresponsible to do so.)

On the other hand, in Section 1.4 we emphasized that there is not always one right answer to an ethical question. Often many responses or actions are ethically acceptable. We also emphasized that there is no algorithm that cranks out the correct answers. We often must use our knowledge of how people behave, what problems have occurred in the past, and so on, to decide what choices are reasonable. Throughout this book we have approached many issues as problem-solving situations. Identity thieves get information in a certain way. How can we make it harder for them while maintaining varied and convenient services for consumers? The Internet exposes children to pornography. How can we reduce that exposure while protecting freedom of speech and access to information for adults? We will see the same approach in some of these ethical scenarios. Rather than concluding that a particular service or product or action is right or wrong, we, as responsible, ethical professionals, look for ways to reduce its negative consequences.

How shall we analyze specific scenarios? We now have a number of tools. We can try to apply our favorite ethical theory, or some combination of the theories. We can ask questions that reflect basic ethical values: Is it honest? Is it responsible? Does it violate an agreement we made? We can consult a code of professional ethics. Ethical theories and guidelines might conflict, or we might find no clause in the Codes specifically applicable. The Preamble of the SE Code, in Appendix A.1, recognizes this problem and emphasizes the need for good judgment and concern for the safety, health, and welfare of the public.

Although we will not follow the outline below step by step for all the scenarios, our discussions will usually include many of these elements:

1. *Brainstorming phase*

- ❖ List all the people and organizations affected. (They are the *stakeholders*.)
- ❖ List risks, issues, problems, and consequences.
- ❖ List benefits. Identify who gets each benefit.
- ❖ In cases where there is no simple yes or no decision, but rather one has to choose some action, list possible actions.

2. *Analysis phase*

- ❖ Identify responsibilities of the decision maker. (Consider responsibilities of both general ethics and professional ethics.)

- ❖ Identify rights of stakeholders. (It might be helpful to clarify whether they are negative or positive rights, in the sense of Section 1.4.3.)
- ❖ Consider the impact of the action options on the stakeholders. Analyze consequences, risks, benefits, harms, costs for each action considered.
- ❖ Find sections of the SE Code or the ACM Code that apply. Consider the guidelines in Section 9.2.3. Consider Kant's and Mill's approaches. Then, categorize each potential action or response as ethically obligatory, ethically prohibited, or ethically acceptable.
- ❖ If there are several ethically acceptable options, select an option, considering the ethical merits of each, courtesy to others, practicality, self-interest, personal preferences, and so on. (In some cases, plan a sequence of actions, depending on the response to each.)

The brainstorming phase can generate a long discussion with humorous and obviously wrong options. In the analysis phase, we might reject some options or decide that the claims of some stakeholders are irrelevant or minor. The brainstorming effort in generating these ideas was not wasted. It could bring out ethical and practical considerations and other useful ideas that one would not immediately think of. And it is as helpful to know why some factors do not carry heavy ethical weight as it is to know which ones do.

9.3.2 PROTECTING PERSONAL DATA

Your customer is a community clinic. The clinic works with families that have problems of family violence. It has three sites in the same city, including a shelter for battered women and children. The director wants a computerized record system, networked for the three sites, with the ability to transfer files among sites and make appointments at any site for any other. She wants to have an Internet connection for routine Web access and e-mail communication with other social service agencies about client needs. She wants a few laptop computers on which staffers can carry records when they visit clients at home. At the shelter, staffers use only first names for clients, but the records contain last names and forwarding addresses of women who have recently left. The clinic's budget is small, and she wants to keep the cost as low as possible.

The clinic director is likely to be aware of the sensitivity of the information in the records and to know that inappropriate release of information can result in embarrassment for families using the clinic and physical harm to women who use the shelter. But she might not be aware of the risks of a computer system. You, as the computer professional, have specialized knowledge in this area. It is as much your obligation to warn the director of the risks as it is that of a physician to warn a patient of side effects of a drug he or she prescribes. (See, for example, ACM Code 1.7 and SE Code 2.07 and 3.12.)

The most vulnerable stakeholders here are the clients of the clinic and their family members, and they are not involved in your negotiations with the director. You, the director, the clinic employees, and the donors or agencies that fund the clinic are also stakeholders.

Suppose you warn the director about unauthorized access to sensitive information by hackers and the potential for interception of records and e-mail during transmission. You suggest measures to protect client privacy, including, for example, an identification code system (not Social Security number) for clients of the clinic to use when real names are not necessary and encryption for e-mail and transmission of records. You recommend security software to reduce the threat of hackers who might steal data. You tell the director that carrying client records on laptops has serious risks, citing examples of loss and theft of laptops containing large amounts of sensitive personal data. You advise that records on laptops be encrypted and suggest that the director buy laptops with thumbprint readers so that only authorized employees can access the data. You warn that staffers might be bribed to sell or release information from the system. (Suppose a client is a candidate for the city council or a party in a child-custody case.) You suggest procedures to reduce such leaks. They include a user ID and password for each staff member, coded to allow access only to information that the particular worker needs, a log function that keeps track of who accessed and modified the records, and monitoring and controls on employee e-mail and Web activity. Note that your ability to provide these suggestions is dependent on your professional competence, currency in the field, and general awareness of relevant current events.

The features you recommend will make the system more expensive. If you convince the director of the importance of your recommendations, and she agrees to pay the cost, your professional/ethical behavior has helped improve the security of the system and protect client privacy.

Suppose the director says the clinic cannot afford all the security features. She wants you to develop the system without them. You have several options. You can develop a cheap, but vulnerable, system. You can refuse and perhaps lose the job (although your refusal might convince the director of the importance of the security measures and change her mind). You can add security features and not charge for them. You can work out a compromise that includes the protections you consider essential. All but the first option are pretty clearly ethically acceptable. What about the first? Should you agree to provide the system without the security you believe it should have? Is it now up to the director alone to make an informed choice, weighing the risks and costs? In a case where only the customer would take the risk, some would say yes, it is your job to inform, no more. Others would say that the customer lacks the professional expertise to evaluate the risks. In this scenario, however, the director is not the only person at risk, nor is the risk to her the most significant risk of an insecure system. You have an ethical responsibility to consider the potential harm to clients from exposure of sensitive information and not to build a system without adequate privacy protection.

The most difficult decision may be deciding what is adequate. Encryption of personal records on the laptops might be essential. Monitoring employee Web access is probably not. There is not always a sharp, clear line between sufficient and insufficient protection. You will have to rely on your professional knowledge, on being up-to-date about current risks and security measures, on good judgment, and perhaps on consulting others who develop systems for similar applications (SE Code 7.08).


Note that, although we have focused on the need for privacy protection here, you can overdo such protection. You also have a professional ethical responsibility not to scare a customer into paying for security measures that are expensive but protect against very unlikely risks.

9.3.3 DESIGNING AN E-MAIL SYSTEM WITH TARGETED ADS

Your company is developing a free e-mail service that will include targeted advertising based on the content of the e-mail messages—similar to Google’s Gmail. You are part of the team designing the system. What are your ethical responsibilities?

Obviously you must protect the privacy of e-mail. The company plans a sophisticated text analysis system to scan e-mail messages and select appropriate ads. No human will read the messages. Marketing for the free e-mail will make clear that users will see targeted ads. The privacy policy will explain that the content of the e-mail will determine which ads appear. So, the marketing director contends, you have satisfied the first principle of privacy protection, informed consent. What else must you consider to meet your ethical responsibility in offering this service to the public?

The fact that software, not a person, scans the e-mail messages and assigns the ads reduces privacy threats. However, we now know that companies store huge amounts of data. What will this system store? Will it store data about which ads it displayed to specific users? Will it store data about which key words or phrases in e-mails cause particular ads to be selected? Will it store data about who clicked on specific ads?

 *Release of search query data: Section 2.1.2* Why are these questions of ethical concern? Because we know that leaks, theft, or demands by a government agency might compromise the privacy of such data. The set of ads displayed to a particular user could provide a lot of information about the person, just as one’s search queries do. Some of it will be incorrect or misleading information because of quirks in the ad-targeting methods.

Should we insist that no such data be stored? Not necessarily. Some of it might have important uses. Some records are necessary for billing advertisers, some for analysis to improve ad-targeting strategies, and perhaps some for responding to complaints from e-mail users or advertisers.

The system design team needs to determine what records are necessary, which need to be associated with individual users, how long the company will store them, how it will

protect them (from hackers, accidental leaks, and so on), and under what conditions it will disclose them.

Now, back up and reconsider informed consent. Telling customers that they will see ads based on the content of their e-mail is not sufficient if the system stores data that can link a list of ads with a particular user. You must explain this to potential users in a privacy policy or user agreement. But we know that most people do not read privacy policies and user agreements, especially long ones. A click might mean legal consent, but ethical responsibility goes farther. Independent of what is in the agreement, the designers must think about potential risks of the system, consider privacy throughout the planning process, and design in protections.

9.3.4 SPECIFICATIONS

You are a relatively junior programmer working on modules that collect data from loan application forms and convert them to formats required by the parts of the program that evaluate the applications. You find that some demographic data are missing from some forms, particularly race and age. What should your program do? What should you do?

Consult the specifications for the program. Any project should have specification documents approved by the client or managers of the company developing the project (or both). Your company has an ethical and business obligation to ensure that the specifications are complete and to produce a program that meets them. Ethical reasons for this include, but go beyond, doing what the company has agreed to do and had been paid to do.

Suppose you do not find anything in the specs that cover your problem. The next step is to bring the problem to the attention of your manager. Suppose the manager tells you “Just make the program assume ‘white’ for race if it’s missing. Banks shouldn’t discriminate based on race anyway.” Do you accept your manager’s decision? You should not. You do not have the authority to make a decision not covered by the specifications without consulting the client or higher level managers in your company who are responsible for the program design. Probably your manager does not either. The manager’s quick and simplistic response suggests that he or she is not acting with informed responsibility. In addition, your company must document whatever decision it makes. That is, the specifications need a revision so that they will be complete (SE Code 3.11).

Why is it important, from an ethical point of view, to consult someone else? Decisions about how a program handles unusual situations might have serious consequences. You (and your manager) might not know enough about the uses of the program to make a good decision. In this example, it is possible that the modules of the program that evaluate the loan application do not use the data on race at all. The lender or the government might want data on race to ensure compliance with nondiscrimination policies and laws.

What other consequences could the manager's decision have? Suppose the company later uses some of your modules in another project, say one that evaluates patients for inclusion in research studies on new drugs. Some diseases and drugs affect people in different ethnic groups differently. Inaccurate data could threaten the health or life of people in the studies and distort the conclusions in ways that harm other people who later use the drugs. But, you might say, we emphasized in Chapter 8 and Section 9.2.3 that people who reuse existing software, especially in a safety critical project, should review the software and its specifications to ensure that it meets the safety standards of the new project. That is their responsibility, you say. But if your way of handling missing data is not in the specifications, how will they know about it? Perhaps someone will notice that the specs are incomplete. Perhaps they will test the modules thoroughly before reusing them and discover what the code does. However, we have seen enough examples of human error to derive a lesson for a responsible professional: Do not count on everyone else to do their jobs perfectly. Do your best to make sure your part is not one of the factors that contribute to a failure.

9.3.5 SKIPPING TESTS

As we observed in Chapter 8, there are often pressures for reducing testing of software. Testing is one of the last steps in development, so when deadlines approach, testing schedules often shrink.

A safety-critical application

Your team is working on a computer-controlled device for treating cancerous tumors. The computer controls direction, intensity, and timing of a beam that destroys the tumor. Various delays have put the project behind schedule, and the deadline is approaching. There will not be time to complete all the planned testing. The system has been functioning properly in the routine treatment scenarios tested so far. You are the project manager, and you are considering whether to deliver the system on time, while continuing testing, and to make patches if the team finds bugs.

The central issue here is safety. Your company is building a machine designed to save lives, but if it malfunctions, it can kill or injure patients. Perhaps the situation seems obvious: Delivering the system on time benefits the company but could endanger the patients—a case of profits versus safety. But we will defer a conclusion until after we analyze the case further.

Who are the people affected? (Who are the stakeholders?) First, the patients who will receive treatment with the machine. A malfunction could cause injury or death. On the other hand, if you delay release of the machine, some patients it might have cured could undergo surgery instead. We will assume treatment with the new machine is preferable because it is less invasive, requires less hospitalization and recovery time,

and overall is less expensive. For some patients, surgery might be impossible, and they could die from their cancer without the new device. Second, there is an impact on the hospitals and clinics who will purchase the machine. Delay could cause financial losses if they have planned on having the machine at the scheduled time. However, it is reasonable for them to expect that the design and testing are professional and complete. You are deceiving the customers if you do not tell them that you have not completed testing. Third, your decision affects you and your company (including its employees and stockholders). Negative consequences of delaying delivery could include damage to your reputation for managing a project (with possible impact on salary and advancement), loss of reputation, a possible fall in stock price for the company, and loss of other contracts, resulting in reduction of jobs for the company's programmers and other employees. As a project manager, you have an obligation to help the company do well. On the other hand, if the system injures a patient, the same negative consequences are likely to occur, in addition to the human feelings of guilt and remorse and significant monetary losses from lawsuits.

This brief examination shows that delivering the system without complete testing could have both negative and positive impacts on patients and also on the manager and the company. The issue is not simply profits versus safety. We assume you are honestly trying to weigh the risks of delivering the system against the costs of delay. However, we must consider a few aspects of human nature that can influence the decision. One is to put more weight on short-term and/or highly likely effects. Many of the costs of delay are fairly certain and immediate, and the risk of malfunction is uncertain and in the future. Also, people tend to use the inherent uncertainties of a situation and the genuine arguments for one side to rationalize making the wrong decision. That is, they use uncertainty to justify taking the easy way out. It might take experience (with both professional and ethical issues), knowledge of cases like the Therac-25, and courage to resist the temptation to put short-term effects ahead of longer-term risks.

Now that we have seen that there are arguments on both sides, we must decide how to weigh them and how to avoid rationalization. First, the machine works well in the routine tests performed so far. The Therac-25 case illustrates that a complex system can function correctly hundreds of times, but fail with fatal consequences in unusual circumstances. Your customer might not know this. You, as a computer professional, have more understanding about the complexity of computer programs and the potential for errors, especially in programs that interact with real-world events such as operator input and control of machinery. We assume that careful thought went into devising the original test plan for the machine. You should delay delivery and complete the tests. (See SE Code 1.03 and 3.10 and ACM Code 1.2.)

Some patients will benefit from on-time delivery. Should their interests bear equal weight with those of the patients whom a malfunction might harm? Not necessarily. The machine represents an improvement in medical treatment, but there is no ethical obligation that it be available to the public on a certain date. You are not responsible for the disease of people who rely on existing treatments. Your obligation to the people who

will use the machine is to be sure that it is as safe as good professional practice can make it, and that includes proper testing. You do not have an ethical obligation to cure people of cancer. You do have an ethical obligation to use your professional judgment in a way that does not expose people, without their knowledge, to additional harm.*

What about your responsibility to your company? Even if we weigh the short-term effects of the delay more highly than the risks of losses that would result from a malfunction, the ethical arguments are on the side of fully testing the machine. Yes, you have a responsibility to help your company be successful, but that is not an absolute obligation. (Recall the discussion of goals and constraints in Section 1.4.3.) Perhaps the distinction would be more obvious if the issue were stealing (from a competitor or a customer perhaps). Your responsibility to the financial success of the company is secondary to ethical constraints. In the present case, avoiding unreasonable risk of harm to patients is the ethical constraint (SE Code 1.02).

Getting a product to market⁶

Most products are not safety-critical ones where flaws might threaten people's lives. Consider this scenario:

You are a programmer working for a very small start-up company. The company has a modest product line and is now developing a truly innovative new product. Everyone is working 60 hour weeks and the target release date is nine months away. The bulk of the programming and testing is done. You are about to begin the beta testing. (See Section 8.3.2 for an explanation of beta testing.) The owner of the company has learned about an annual industry show that would be ideal for introducing the new product. The show is in two months. Packaging must start within a week in order to have the product on the shelves for the show. The owner talks with the project manager. They decide to skip the beta testing and start making plans for an early release.

Should you protest? Students discussing this scenario generally recognize that the decision is a bad one and that the company should do the beta testing. They ask, however, if the programmer is even in a position to protest. Are you supposed to do what the project manager, your direct supervisor, says? Should you say nothing, speak up, or quit?

Consider this possible outcome: The programmer asks for a meeting with the owner. He explains that the product is not ready, that beta testing is a very important stage of development, and they should not skip it. The owner (who is not a programmer) accepts what the programmer tells him and drops the idea of an early release. The new product, released when originally planned, is a success. The programmer eventually becomes the head of quality control for the growing company.

*There are many situations where patients knowingly try risky drugs or treatments. Here, we are assuming that doctors and hospitals do not present the device as risky or experimental but as a new, presumably safe, treatment device.

This is not a fairy tale. It is an actual case, and the outcome I just described is what actually happened. This case makes a very important point: Sometimes people will listen to you, provided, of course, you are respectful, thoughtful, and well prepared. In another actual case, a manager within a company, but not in the software division, asked a programmer to do something the programmer knew was not a good idea. Although she feared that she might lose her job for refusing a manager's request, she said no and gave a brief explanation. The manager accepted the explanation, and that was the end of the incident. People often ask for things they do not necessarily expect to get. It is important to keep in mind that others might respect your opinion. You might be the only one who recognizes the problem or understands a particular situation. Your responsibilities to your company include applying your knowledge and skill to help avoid a bad decision. In the start-up scenario, speaking up might have had a significant impact on the success of the product and the company. Many people are reasonable and will consider a good explanation or argument. Of course, not all cases end this well.

The CEO of a small electronics company proposed producing a new version of a product within three months. The director of engineering (an excellent, experienced software engineer) wrote up a detailed schedule of all the necessary steps and told the CEO that the project would take more than a year. Note that the software engineer did not simply tell the CEO that the three-month plan was unreasonable. He documented his claim. (SE Code 2.06 and 3.09 apply.) The CEO replaced him with someone who had a "can do" attitude. This is one of many cases where doing what is professionally responsible corresponds with doing what is good for oneself. The software engineer did not want the stress of working under an extremely unreasonable schedule and the responsibility for the inevitable failure. Leaving the company was not a bad thing.

9.3.6 COPYRIGHT VIOLATION

Your company has 25 licenses for a computer program, but you discover that it has been copied onto 80 computers.

The first step here is to inform your supervisor that the copies violate the license agreement. Suppose the supervisor is not willing to take any action? What next? What if you bring the problem to the attention of higher level people in the company and no one cares? There are several possible actions: Give up; you did your best to correct the problem. Call the software vendor and report the offense. Quit your job.

Is giving up at this point ethically acceptable? My students thought it depended in part on whether you are the person who signed the license agreements. If so, you have made an agreement about the use of the software, and you, as the representative of your company, are obligated to honor it. Because you did not make the copies, you have not broken the agreement directly, but you have responsibility for the software. Your name on the license could expose you to legal risk, or unethical managers in your company could make you a scapegoat. Thus, you might prefer to report the violation or quit your job and have your name removed from the licenses to protect yourself. If you are not the person

who signed the licenses, then you observed a wrong and brought it to the attention of appropriate people in the company. Is that enough? What do Sections 2.02, 6.13, and 7.01 of the SE Code and 1.5 and 2.6 of the ACM Code suggest?

9.3.7 GOING PUBLIC

Suppose you are a member of a team working on a computer-controlled crash-avoidance system for automobiles. You think the system has a flaw that could endanger people. The project manager does not seem concerned and expects to announce completion of the project soon. Do you have an ethical obligation to do something?

Given the potential consequences, yes (see SE Code 1.04; ACM Code 1.2, 2.5). We consider a variety of options. First, at a minimum, discuss your concerns with the project manager. Voicing your concerns is admirable and obligatory. It is also good for your company. Internal “whistle-blowing” can help protect the company, as well as the public, from all the negative consequences of releasing a dangerous product. If the manager decides to proceed as planned with no examination of the problem, your next option is to go to someone higher up in the company.

If no one with authority in the company is willing to investigate your concerns, you have a more difficult dilemma. You now have the option of going outside the company to the customer, to the news media, or to a government agency. There is personal risk of course: You might lose your job. There is also the ethical issue of the damage you might do to your company, and ultimately to the people who would benefit from the system. You might be mistaken. Or you might be correct, but your method of whistle-blowing might produce negative publicity that kills a potentially valuable and fixable project. As the ACM Code (1.2) says, “misguided reporting of violations can, itself, be harmful.” At this point it is a good idea to consider whether you are confident that you have the expertise to assess the risk. It could help to discuss the problem with other professionals. If you conclude that the management decision was an acceptable one (and that you are not letting your concern for keeping your job sway your conclusion), this might be the point at which to drop the issue. If you are convinced that the flaw is real, or if you are aware of a careless, irresponsible attitude among the company managers, then you must go further (SE Code 6.13). You are not an uninvolved bystander, for whom the question of ethical obligation might be more fuzzy. The project pays your salary. You are part of the team; you are a participant. Note also that this is the kind of situation suggested in the SE Code 2.05, where you may violate a confidentiality agreement.

There have been several dramatic cases where professionals faced this difficult situation. Computer engineers who worked on the San Francisco Bay Area Rapid Transit system (BART) worried about the safety of the software designed to control the trains. Although they tried for many months, they were not successful in their attempts to convince their managers to make changes. Eventually, a newspaper published some of their

critical memos and reports. The engineers were fired. During the next few years, when several crashes occurred, there were public investigations and numerous recommendations made for improving safety of the system.⁷

One of the BART engineers made these comments about the process:

If there is something that ought to be corrected inside an organization, the most effective way to do it is to do it within the organization and exhaust all possibilities there . . . you might have to go to the extreme of publishing these things, but you should never start that way.⁸

It is important, for practical and ethical reasons, to keep a complete and accurate record of your attempts to bring attention to the problem and the responses from the people you approach. The record protects you and others who behave responsibly and could help avoid baseless accusations later.

9.3.8 RELEASE OF PERSONAL INFORMATION

We will look at two related scenarios. Here is the first:

You work for the IRS, the Social Security Administration, a movie-rental company, or an Internet service provider. Someone asks you to get a copy of records about a particular person. He will pay you \$500.

Who are the stakeholders? You: You have an opportunity to make some extra money. The person seeking the records: Presumably he has something to gain. The person whose records the briber wants: Providing the information invades his or her privacy. All the people about whom the company or agency has personal information: If you sell information about one person, chances are you will sell more if asked in the future. Your employer (if a private company): If the sale becomes known, the victim might sue the company. If such sales of information become common, the company will acquire a reputation for carelessness and will potentially lose business and lawsuits.

There are many alternative actions open to you: Sell the records. Refuse and say nothing about the incident. Refuse and report the incident to your supervisor. Refuse and report to the police. Contact the person whose information the briber wants and tell him or her of the incident. Agree to sell the information, but actually work with the police to collect evidence to convict the person trying to buy it.

Are any of these alternatives ethically prohibited or obligatory? The first option, selling the records, is clearly wrong. It almost certainly violates rules and policies you have agreed to abide by in accepting your job. As an employee, you must abide by the guarantees of confidentiality the company or agency has promised its customers or the public. Depending on the use made of the information you sell, you could be helping to cause serious harm to the victim. Disclosing the information might be illegal. Your action might expose your employer to fines. If someone discovers the leak, the employer

and the police might suspect another employee, who could face arrest and punishment. (See ACM Code: 1.2, 1.3, 1.7, 2.6; SE Code: 2.03, 2.05, 2.09, 4.04, 6.05, 6.06.)

Some would argue that selling the records is wrong because it violates the privacy of the victim, but recall that the boundaries of privacy are unclear because they can conflict with freedom of speech and reasonable flow of information. If you happened to know the victim, and knew some of the same information in the records, you might not be under an ethical obligation to keep the information secret. The essential element that makes selling the information wrong in this scenario is your position of trust as an employee in a company or agency that maintains the information. The risks are greater for sensitive information, but your obligation extends to any information the company has promised to keep confidential.

What about the second alternative: refusing to provide the records, but not reporting the incident? Depending on policies of the employer (and laws related to certain government agencies; see SE Code 6.06 and ACM Code 2.3), you might be obligated to report any attempt to gain access to the records. There are other good reasons for reporting the incident. Reporting could lead to the capture of someone making a business of buying sensitive information without the knowledge or consent of the person the information concerns and without the knowledge and consent of the companies and agencies responsible for the information. It could protect you and other innocent employees if someone later discovers the sale of the records and does not know who sold them. (Some ethicists, for example, deontologists, argue that taking an action because it benefits you is not ethically meritorious. However, one can argue that taking an action that protects an innocent person is meritorious, even if the person is yourself.)

ACM Code 1.2 and 1.7 suggest an obligation to report, but it is not explicit. There might be disagreement about whether you are ethically bound to do more than refuse to sell the information. It is difficult to decide how much you must do to prevent a wrong thing from happening if you are not participating in the wrong act. A recluse who ignores evils and pains around him might not be doing anything unethical, but he is not what we would consider a good neighbor. Acting to prevent a wrong is part of being a good neighbor, good employee, or good citizen—it is ethically admirable—even in situations where it is not ethically obligatory.

Now consider a variation of this scenario.

You know another employee sells records with people's personal information.

Your options include doing nothing, talking to the other employee and trying to get him or her to stop selling files (by threats of exposure or ethical arguments), reporting to your supervisor, or reporting to an appropriate law-enforcement agency. The question here is whether you have an obligation to do anything. This scenario differs from the previous one in two ways. First, you have no direct involvement; no one has approached you. This difference might seem to argue for no obligation. On the other hand, in the first scenario, if you refused to sell the file, the buyer might give up, and the victim's information would remain protected. In this case, you know that a sale of confidential, sensitive information

occurred. Thus the argument in favor of an obligation to take action is stronger (see SE Code 6.13 and 7.01).

9.3.9 CONFLICT OF INTEREST

You have a small consulting business. The CyberStuff company plans to buy software to run a new collaborative content-sharing Web site. CyberStuff wants to hire you to evaluate bids from vendors. Your spouse works for NetWorkx and did most of the work in writing the bid that NetWorkx plans to submit. You read the bid while your spouse was working on it and you think it is excellent. Do you tell CyberStuff about your spouse's connection with NetWorkx?

Conflict-of-interest situations occur in many professions. Sometimes the ethical course of action is clear. Sometimes, depending on your connection with the people or organizations your action affects, it can be more difficult to determine.

I have seen two immediate reactions to scenarios similar to this one (in discussions among professionals and among students). One is that it is a simple case of profits versus honesty, and ethics requires that you inform the company about your connection to the software vendor. The other is that if you honestly believe you can be objective and fairly consider all bids, you have no ethical obligation to say anything. Which is right? Is this a simple choice between saying nothing and getting the consulting job or disclosing your connection and losing the job?

The affected parties are the CyberStuff company, yourself, your spouse, your spouse's company, and the other companies whose bids you will be reviewing. A key factor in considering consequences is that we do not know whether CyberStuff will later discover your connection to one of the bidders. If you say nothing about the conflict of interest, you benefit, because you get the consulting job. If you recommend NetWorkx (because you believe its bid is the best), it benefits from a sale. However, if CyberStuff discovers the conflict of interest later, your reputation for honesty—important to a consultant—will suffer. The reputation of your spouse's company could also suffer. Note that even if you conclude that you are truly unbiased and do not have an ethical obligation to tell CyberStuff about your connection to your spouse's company, your decision might put NetWorkx's reputation for honesty at risk. The appearance of bias can be as damaging (to you and to NetWorkx) as actual bias.

Suppose you take the job and you find that one of the other bids is much better than the bid from NetWorkx. Are you prepared to handle that situation ethically?

What are the consequences of disclosing the conflict of interest to the client now? You will probably lose this particular job, but they might value your honesty more highly and that might get you more business in the future. Thus, there could be benefits, even to you, from disclosing the conflict of interest.

Suppose it is unlikely that anyone will discover your connection to NetWorkx. What are your responsibilities to your potential client as a professional consultant? When

someone hires you as a consultant, they expect you to offer unbiased, honest, impartial professional advice. There is an implicit assumption that you do not have a personal interest in the outcome or a personal reason to favor one of the bids you will review. The conclusion in this case hangs on this point. In spite of your belief in your impartiality, you could be unintentionally biased. It is not up to you to make the decision about whether you can be fair. The client should make that decision. Your ethical obligation in this case is to inform CyberStuff of the conflict of interest. (See SE Code Principle 4, 4.03, and 4.05, and ACM Code 2.5.)

9.3.10 KICKBACKS AND DISCLOSURE

You are a programmer on the programming staff of a major university. The office that plans freshman orientation is selecting one or two brands of security software for laptops and cell phones to recommend to all new students. Your supervisor has asked you to evaluate software from a dozen companies and make recommendations. One of the companies takes you out to dinner, gives you free software (in addition to the security software you are evaluating), offers to pay your expenses to attend a professional conference on computer security, and offers to give the university a percentage of the price for every student who buys its security package.

You are sensitive to the issue of bribery, but the cost of the dinner and software the company gave you is relatively small. The university cannot pay to send you to conferences. Attending one will improve your knowledge and skills and make you better at your job, a benefit to both you and the university. The percentage from the sales benefits the university and thus all the students. This sounds like a good deal for all.

It also might sound a bit familiar. Universities recommend loan companies to students seeking student loans. A flurry of news reports disclosed that several universities and their financial-aid administrators gave special privileges and preferred recommendations to particular lending companies in exchange for payments to the universities and consulting fees, travel expenses, and other gifts for the administrators. Some financial aid officers defended the practices. Professional organizations scurried to write new ethical guidelines. Some lenders paid heavy fines. The reputations of the universities suffered. The government heavily regulates the lending industry, so we return to the security software scenario to discuss ethical issues, not primarily legal ones.

First of all, does your employer have a policy about accepting gifts from vendors? Even if gifts appear small to you and you are confident that they do not influence your judgment, you are obligated to follow your employer's policy. Violating the policy violates an agreement you have made. Violating the policy could expose the employer to negative publicity (and possibly legal sanctions). (See SE Code 6.05 and 6.06. SE Code 1.06, 4.03, and 4.04 are also relevant to this case.)

Who does not benefit from the arrangement with the software company? Any company that charges less for software of comparable quality. Any company that charges

the same or perhaps a little more for a better product. All the students who rely on the recommendation. The university's obligation in making the recommendation is primarily to the students. Will the benefits the programmer and university receive sway their choice of company to the point where they do not choose the product best for the students?

People want to know when a recommendation represents an honest opinion and when someone is paying for it. We expect universities and certain other organizations to be impartial in their recommendations. When a programmer selects software to recommend, the presumption is that it is, in the programmer's opinion, the best for the buyer. If there are other reasons for the selection, the programmer should disclose them. Disclosure is a key point. Many organizations encourage their members to get a credit card that provides a kickback to the organization. This is not unethical primarily because the kickback is made clear. It is even a selling point: Use this card and help fund our good cause. However, even if the university makes clear in its recommendation that it benefits financially from sales of the product, there are good arguments against the arrangement. They are not computer professional issues, so we leave them for you to think about.

9.3.11 A TEST PLAN

A team of programmers is developing a communications system for firefighters to use when fighting a fire. Firefighters will be able to communicate with each other, with supervisors near the scene, and with other emergency personnel. The programmers will test the system in a field near the company office.

What is the ethical issue? The test plan is insufficient and this is an application where lives could be at risk. Testing should involve real firefighters inside buildings or in varied terrain, perhaps in an actual fire (perhaps a controlled burn). The programmers who work on the system know how it behaves. They are experienced users with a specific set of expectations. They are not the right people to test the system. Testing must address issues such as: Will the devices withstand heat, water, and soot? Can someone manipulate the controls wearing heavy gloves? Are the controls clear and easy to use in poor light conditions? Will a building's structure interfere with the signal?

In an actual case, the New York City fire commissioner halted use of a \$33 million digital communications system after a fireman called for help on his radio and no one heard. Firefighters reported other problems during simulation tests. The commissioner commented "We tested the quality, durability, and reliability of the product, but we didn't spend enough time testing them in the field or familiarizing the firefighters with their use."⁹

9.3.12 ARTIFICIAL INTELLIGENCE AND SENTENCING CRIMINALS

You are part of a team developing a sophisticated program using artificial intelligence (AI) techniques to make sentencing decisions for convicted criminals.

Maybe, in the future, we will have computer systems capable of doing this well without human intervention. It is helpful for judges to review sentencing in cases with similar characteristics, but judges use their discretion in deciding sentences (within bounds established in law). Prosecutors and defense lawyers present arguments that a judge considers, but software cannot. A judge can consider unusual circumstances in the case, characteristics of the convicted person, and other factors that a program cannot handle. Judges sometimes innovate creative new aspects of sentencing. A program that analyzes and chooses from prior cases cannot. On the other hand, some judges have a reputation for giving extremely tough sentences, while others are very lenient. Some people argue that software might be more fair than a judge influenced by personal impressions and biases. At this point, however, most of the legal community, and probably the public, would prefer to have human judges make sentencing decisions. Years of experience provide insights that are, at this time, difficult to encode into software. For now, we modify the scenario by adding two words:

You are part of a team developing a sophisticated program using AI techniques to help judges make sentencing decisions for convicted criminals.

The system will analyze characteristics of the crime and the criminal to find other cases that are similar. Based on its analysis of cases, should it then make a recommendation for the sentence in the current case, or should it simply display similar cases, more or less as a search engine would, so that the judge can review them? Or should it provide both a recommended sentence and the relevant cases?

This is clearly an application where it is essential to have experts and potential users involved in the design. The expertise and experience of judges and lawyers are essential for choosing criteria and strategies for selecting the similar cases on which the program bases its recommendation or on which a judge bases a decision. The system's recommendations, if it makes them, must comply with sentencing requirements specified in laws.

The involvement of lawyers can improve more subtle decisions. Consider the question of the ordering of the cases the system displays. Should it order them by date or by the length of the sentence? If the latter, should the shortest or longest sentences come first? This last question suggests that the project's consultants should include both prosecutors and defense lawyers. But probably none of these orderings is best. Perhaps you should order the cases according to an evaluation of their similarity or relevance to the current case. That is a fuzzier criterion than date or length of sentence. Again, it is important to include a variety of experts, with different perspectives, in the design process.

Is the ordering of the selected cases so important? When you are researching some topic, how many pages of search-engine results do you look at? Many people rarely go beyond the first page. We expect a judge making a sentencing decision to be more thorough. Experience and human factors research, however, remind us that people sometimes are tired or rushed. Sometimes they have too much confidence in results

from computer systems. (We saw examples in Chapter 8. County election officials and school districts ignored warnings that they should not rely solely on results from computer systems when making decisions about voter eligibility and about assigning students to summer school.) Even when people are deliberate and careful in interpreting output from a computer system, the manner in which the viewers see the data can influence their perceptions. Thus careful planning, including much consultation with relevant experts, is an ethical requirement in a system that will have significant impact on people's lives.

A company or government agency that develops or installs this system must consider how it will maintain and update the system. Clearly there will be new cases to add. How will the system handle changes in sentencing laws? Should it discard cases decided under the old law? Include them but flag them clearly as predating the change? How much weight should the system give such cases in its selection criteria?

We have not yet answered the question about whether the system should recommend a sentence. A specific recommendation from the system that differs from the judge's initial plan might lead a judge to give a case more thought. Or it might influence a judge more than it should. If the system presents a recommendation, legislators or administrators might begin to think that a clerk or law student, not a judge, can operate the system and handle sentencing. This is not likely in the short term—judges and lawyers would object. It is, however, a possible consequence of apparently sophisticated AI systems making apparently wise decisions in any professional area. A potential drop in employment for judges (or other professionals) is not the main issue. The quality of the decisions is. Thus an answer to the question will depend in part on the quality of AI technology (and the specific system) at the time of development and on the sensitivity of the application. (See Exercise 6.27 for another application area.)

Suppose judges in your state use a sentencing decision system that displays similar cases for the judge to review. You are a programmer working for your state government. Your state has just made it a criminal offense to use a cell phone while taking a college exam. Your boss, a justice department administrator, tells you to modify the program to add this new category of crime and assign the same relevancy weights to cases as the program currently does for using a cell phone while driving a car (already illegal in your state).

The first question, one for your boss, is whether the contract under which the system operates allows the state to make changes. For many consumer products, guarantees and service agreements become void if the consumer takes the product apart and makes changes. The same can be true for software. Let us assume the boss knows that the state's contract allows the state to modify the system.

Suppose you know that your boss made the decision quickly and independently. You should say no, with appropriate politeness and reasons. SE Code 3.15 states a very important, often ignored principle: "Treat all forms of software maintenance with the same professionalism as new development." That includes developing specifications, in

this example in consultation with lawyers and judges who understand the law and its subtleties. We raised a sampling of the complex and sensitive issues that go into the design of a system such as this. Modifications and upgrades should undergo as thorough planning and testing.

9.3.13 A GRACIOUS HOST

You are the computer system administrator for a mid-sized company. You can monitor the company network from home, and you frequently work from home. Your niece, a college student, is visiting for a week. She asks if she can use your computer to check her e-mail. Sure, you say.

You are being a gracious host. What is the ethical problem?

Maybe there is none. Maybe you have an excellent firewall and excellent antivirus software. Maybe your files are password protected, and you created a separate account on your computer for your niece. But maybe you did not even think about security when your niece asked to use the computer.

Your niece is a responsible person. She would not intentionally snoop or harm you or your company. But after checking e-mail, she might visit MySpace, then look for someone selling cheap concert tickets, then ... who knows? Maybe her own computer crashed twice in the past six months because of viruses.

Your company network contains employee records, customer records, and plenty of information about company projects, finances, and plans. Depending on what the company does, the system might contain other very sensitive information. Downtime, due to a virus or similar problem, would be very costly for the company. In an actual incident, someone in the family of a mortgage company employee signed up for a peer-to-peer file sharing service and did not properly set the options indicating which files were to be shared. Mortgage application information for a few thousand customers leaked and spread on the Web.

The point of this scenario is that you must always be alert to potential risks. Mixing family and work applications poses risks.

EXERCISES

Review Exercises

- 9.1 What are two ways professional ethics differ from ethics in general?
- 9.2 Why did a program to read handwriting, developed by Microsoft programmers, fail?
- 9.3 What is one important policy decision a company should consider when designing a system to target ads based on e-mail content?
- 9.4 You are a programmer, and you think there is a serious flaw in software your company is developing. Who should you talk to about it first?

General Exercises

- 9.5 Describe a case at work or in school where someone asked or pressured you to do something you thought unethical.
- 9.6 Review the description of the airplane crash near Cali, Columbia in Section 8.3.2. Find specific guidelines in Section 9.2.3 and the ethics codes in Appendix A that, if followed carefully, might have avoided problems in the flight-management software that contributed to the crash.
- 9.7 You are setting up a small business with a Web site and considering what privacy policy to adopt for the information you will collect about your customers. You will choose either informed consent (stating how you use the information, with no opt-out options), an opt-out option, or opt-in box to click (as described in Section 2.1.3). Your site will clearly and fully explain your policy. Are any of the three choices ethically obligatory or ethically prohibited, or are all ethically acceptable? Justify your answers.
- 9.8 The management team of a cell phone service company is debating options for customer retrieval of their voice-mail messages. Some managers argue to provide quick retrieval, that is, access to messages without a PIN when the system recognizes that the call is coming from the customer's own phone. Some managers argue that this should be an option the customer can turn on or off. Others argue that the company should always require the PIN because most people do not know about the risk of Caller ID spoofing. (That is, someone else can call in and trick the company's system into believing the call is coming from the customer's phone.)
From an ethical point of view, which of these options (or others you might think of) are ethically acceptable? Which is best? (The methodology of Section 9.3.1 might be helpful to the analysis.)
- 9.9 Suppose the cell phone service company in the previous exercise chooses to provide quick retrieval of messages without a PIN as an option. What should the default setting for this option be when someone initiates service? Why?
- 9.10 A factory manager has hired your company to develop and install a surveillance system in the factory. The system includes cameras small enough not to be noticed. Supervisors and security personnel can view images in real time on monitors in a control room. The system will store the video. The factory manager says the purposes are to watch for safety problems and for theft of materials by workers. What issues, specifications, and policies will you discuss with the manager? Would you set any conditions on taking the job? Explain.
- 9.11 You work for a company that develops security products. You helped write software for a car door lock that operates by matching the driver's thumbprint. The manager for that project is no longer at the company. A local power station wants your company to develop a thumbprint-operated lock for secure areas of the power station. Your boss says to use the software from the car locks. What is your response?
- 9.12 Write a scenario to illustrate SE Code 2.05 and ACM Code 1.8.
- 9.13 You are a manager at a health-maintenance organization. You find that one of your employees has been reading people's medical records without authorization. What is your response?
- 9.14 In many cities, wills processed by courts are public records. A business that sells information from local public records is considering adding a new "product," lists of people who recently inherited a large amount of money. Using the methodology of Section 9.3.1, analyze the ethics of doing so.
- 9.15 You are designing a database to keep track of patients while they are in a hospital. The record for each patient will include special diet requirements. Describe some approaches to deciding how to

- design the list of diet options from which a user will select when entering patient data. Evaluate different approaches.
- 9.16 You are offered a job with a company that is developing software for a new generation of space shuttles. You do not have any training in the specific techniques used in the programs you will be working on. You can tell from the job interview that the interviewer thinks your college program included this material. Should you take the job? Should you tell the interviewer that you have no training or experience in this area? Analyze this scenario, using the methods in Section 9.3.1. Find relevant sections from the ethics codes in Appendix A.
- 9.17 You are a programmer for a company that manages large investment portfolios. You have been working on a project to develop a program to decide how to invest a large amount of money according to criteria that balance risk and potential gain according to the client's preferences. The program is complete and has performed well in preliminary testing, but the planned full-scale testing has not yet been done. It is Friday afternoon, and one of the investment managers has just received a large amount of money from a client to invest. The investment manager wants to get the money into the stock market before the weekend. He tells you that there is not enough time to use the old investment-planning method. He wants a copy of your program to run. Your supervisor, the software manager, has gone away for the weekend. What do you do? Analyze this scenario, using the methods in Section 9.3.1.
- 9.18 A small company offers you a programming job. You are to work on new versions of its software product to disable copy-protection and other access controls on electronic books. The company's program enables buyers of e-books to read their e-books on a variety of hardware devices (fair uses). Customers can also use the program to make many unauthorized copies of copyrighted books. The company's Web page implicitly encourages this practice. Analyze the ethics of accepting the job. Find relevant sections from the ethics codes in Appendix A. (For this exercise, assume you are in a country that does not outlaw tools to circumvent copy protection as the Digital Millennium Copyright Act does in the United States.)
- 9.19 Find at least two examples described in this book where there was a violation of Clause 3.09 of the SE Code.
- 9.20 Clause 1.03 of the SE Code says "Approve software only if" it does not "diminish privacy or harm the environment." Search engines can diminish privacy. Do they violate this clause? Should the clause say something about trade-offs, or should we interpret it as an absolute rule? The concluding sentence of Clause 1.03 says, "The ultimate effect of the work should be to the public good." Does this suggest trade-offs? Give another example in which the dilemma in this exercise would be relevant.
- 9.21 Clause 8.07 in the SE Code says we should "not give unfair treatment to anyone because of any irrelevant prejudices." The guidelines for Section 1.4 of the ACM Code say "Discrimination on the basis of ... national origin ... is an explicit violation of ACM policy and will not be tolerated." Analyze the ethical issues in the following scenario. Do you think the decision in the scenario is ethically acceptable? How do the relevant sections from the two Codes apply? Which Code has a better statement about discrimination? Why?

Suppose you came to the U.S. from Iraq 15 years ago. You now have a small software company. You will need to hire six programmers this year. Because of the devastation by the war in your homeland, you have decided to seek out and hire only programmers who are refugees from Iraq.

9.22 Consider the following statements.

1. In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.¹⁰
2. We cannot assume that a computer-based economy automatically will provide enough jobs for everyone in the future. Computer professionals should be aware of this pressure on employment when designing and implementing systems that will reduce job opportunities for those most in need of them.¹¹

Compare the two statements from the perspective of how relevant and appropriate they are for an ethical code for computer professionals. Do you think both should be in such a code? Neither? Just one? (Which one?) Give your reasons.

- 9.23 You are the president of a small computer-game company. Your company has just bought another small game company that was developing three new games. You look them over and find that one is complete, ready to reproduce and sell. It is very violent and demeaning to women. It would probably sell 200,000–400,000 copies. You have to decide what to do with the game. Give some options, and give arguments for and against them. What will you do? Why?
- 9.24 Suppose there are two large competing telecommunications firms in your city. The companies are hostile to each other. There have been unproven claims of industrial espionage by each company. Your spouse works for one of the companies. You are now interviewing for a job with the other. Do you have an ethical obligation to tell the interviewer about your spouse's job? How is this case similar to and different from the conflict-of-interest case in Section 9.3.9?
- 9.25 A Dutch hacker who copied patient files from a University of Washington medical center (and was not caught) said in an online interview that he did it to publicize the system's vulnerability, not to use the information. He disclosed portions of the files (to an individual, not the public) after the medical center said that no patient files had been copied.¹² Analyze the ethics of his actions using the methodology of Section 9.3.1. Was this honorable whistle-blowing? Irresponsible hacking?
- 9.26 Consider the scenario in Section 9.3.5. Suppose that the company has decided to deliver the device before completing the testing and that you have decided you must inform the hospitals that are purchasing it. Discuss ethical arguments about whether to include your name with the information you give to the hospitals or to send it anonymously.
- 9.27 The first case in Section 9.3.5 concerns safety-critical systems. Suppose the software product in the second scenario is an accounting system, or a game, or a photo-sharing system for the Web. Which principles or ideas in the analysis of the first scenario apply to the second one? Which do not? Explain your answers.
- 9.28 The scenario in Section 9.3.7 concerns going public about possible flaws in a safety-critical application that can cause injury or death. For what other kinds of applications, if any, not including risks to health and life, do you think it would be appropriate to go public about potential flaws that management is unwilling to correct?
- 9.29 You run a small company that developed and markets a filter program that enables parents to block access to Internet sites they do not want their children to visit. A large corporation has asked you to customize the program to install on its machines to block access by employees to

various game sites, sites containing pornography, and video-sharing sites. A foreign government has asked you to customize the program to install on its Internet gateways to block access by people in the country to sites containing pornography and sites containing political discussion critical of the government.

Will you accept either or both jobs? If one but not the other, make clear the reasons for the distinction.

- 9.30 Several professional associations of engineers opposed increased immigration of skilled high-tech workers. Was this ethical? Give arguments for both sides. Then give your view and defend it.

Assignments

These exercises require some research or activity.

- 9.31 Watch a science fiction movie set in the near future. Describe a computer or telecommunications system in the movie that does not currently exist. Suppose, in the years before the movie takes place, you are on the team that develops it. Identify issues of professional ethics the team should consider.

Class Discussion Exercises

These exercises are for class discussion, perhaps with short presentations prepared in advance by small groups of students.

- 9.32 You are the programmer in the clinic scenario (Section 9.3.2). The director has asked you to rank your suggestions for security and privacy protection measures so that she can choose the most important ones while still trying to stay within her budget. Group the suggestions into at least three categories: essential, recommended, and least important. Include explanations you might give her and assumptions you make (or questions you would ask her) to help determine the importance of some features.
- 9.33 You are an experienced programmer working on part of a project to enable people to control household appliances from their cell phone. (For example, they can turn on the air-conditioning while on the way home.) You have figured out that you can do a part of your section of the program in a way that is more efficient than the method described in the specifications. You are confident that your method is correct, and you know that the change will have no impact on other parts of the program. You understand the importance of following specifications, but you also know that any proposed revision generates a long, bureaucratic process that will take weeks and require approvals from many people in both your company and the client company. Is this a case where the trade-offs make it reasonable to use the better method without a revision of the specifications? Explain your response.
- 9.34 The faculty at a large university requested that the campus store sell an electronic device, AutoGrader, that students would use when taking machine-scorable tests. Students would enter test answers into this personal electronic device. When done, they send the answers via infrared signal to the instructor's computer in the classroom. Once the instructor's computer receives the answers, it immediately grades the test and sends each student's score back to the student's device.

Suppose you are a university dean who must decide whether to allow use of this system. Analyze the decision as both an ethical and practical problem. Discuss potential benefits and

problems or risks of using the system. Discuss all the issues (of the kind relevant to the topics of this book) that are relevant to making the decision. Mention any warnings or policies you might include if you approve use of the system.

- 9.35 As we saw in Section 7.5.3, many people, including Sun Microsystems cofounder Bill Joy, fear that development of intelligent robots could have devastating consequences for the human race.¹³ Is it ethical to do research aimed at improving artificial intelligence?



NOTES

1. The full names are the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers.
2. Bob Davis and David Wessel, *Prosperity: The Coming 20-Year Boom and What It Means to You* (Random House, 1998), p. 97.
3. Charles Piller, “The Gender Gap Goes High-Tech,” *Los Angeles Times*, August 25, 1998, p. A1.
4. Bill Gates, *The Road Ahead* (Viking, 1995), p. 78.
5. Roger Boisjoly, quoted in Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (University of Chicago Press, 1996), p. 41.
6. I thank Cyndi Chie for giving me this scenario.
7. Robert M. Anderson et al., *Divided Loyalties: Whistle-Blowing at BART* (Purdue University, 1980).
8. Holger Hjørsvang, quoted in Anderson et al., *Divided Loyalties*, p. 140.
9. Robert Fox, “News Track,” *Communications of the ACM*, 44, no. 6 (June 2001), pp. 9–10; Kevin Flynn, “A Focus on Communication Failures,” *New York Times*, January 30, 2003, p. A13.
10. Guidelines of the ACM Code of Ethics and Professional Conduct (Section 1.1).
11. Tom Forester and Perry Morrison, *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*, 2nd ed. (MIT Press, 1994), p. 202.
12. Marc L. Songini, “Hospital Confirms Copying of Patient Files by Hacker,” *Security Informer*, December 14, 2000 (accessed June 4, 2001). The article is no longer accessible on the Security Informer Web site. A version of it from *Computerworld*, dated December 15, 2000, is at archives.cnn.com/2000/TECH/computing/12/15/hospital.hacker.idg (accessed April 20, 2007).
13. Bill Joy, “Why the Future Doesn’t Need Us,” *Wired*, April 2000, www.wired.com/wired/archive/8.04 (accessed September 6, 2007).



BOOKS AND ARTICLES

- Anderson, Robert M., Robert Perrucci, Dan E. Schendel, and Leon E. Trachtman. *Divided Loyalties: Whistle-Blowing at BART*. Purdue University, 1980.
- Anderson, Ronald E., Deborah G. Johnson, Donald Gotterbarn, and Judith Perrolle. “Using the New ACM Code of Ethics in Decision Making.” *Communications of the ACM*, 36, no. 2 (February 1993): 98–107.
- Bayles, Michael D. *Professional Ethics*. Wadsworth, 1981.
- Cerf, Vint. “Ethics and the Internet.” *Communications of the ACM*, 32, no. 6 (June 1989): 710. An early attempt to establish a standard of ethics for the Internet.
- Collins, W. Robert, Keith W. Miller, Bethany J. Spielman, and Phillip Wherry. “How Good Is Good Enough?” *Communications of the ACM*, 37, no. 1 (January 1994): 81–91.

- Ermann, M. David, Mary B. Williams, and Michele S. Shauf, eds. *Computers, Ethics and Society*. 2nd ed. Oxford University Press, 1997.
- Gotterbarn, Donald, Keith Miller, and Simon Rogerson. "Software Engineering Code of Ethics Is Approved." *Communications of the ACM*, 42, no. 10 (October 1999): 102–107.
- Johnson, Deborah G. *Computer Ethics*. 3rd ed. Prentice Hall, 2001.
- Rachels, James. *The Elements of Moral Philosophy*. McGraw Hill, 1993.
- Spinello, Richard. *CyberEthics: Morality and Law in Cyberspace*. Jones and Bartlett, 2000.
- Vaughan, Diane. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. University of Chicago Press, 1996.



ORGANIZATIONS AND WEB SITES

- ACM: www.acm.org
- Computer Professionals for Social Responsibility: cpsr.org
- IEEE Computer Society: www.computer.org