10.1 Ethics

10.1.1 What is "Computer Ethics"?

In the previous chapters, we discussed issues and problems related to computers from a somewhat detached perspective. We saw how a new technology can create new risks and problems and how social and legal institutions must continually adapt. But technology is not an inevitable force, outside of human control. People make decisions about what technology and products to develop and how to use them. People make decisions about when a product is safe to release. People make decisions about access to and use of personal information. People make laws and set rules and standards. In this chapter, we look at those decisions and activities from an ethical perspective. We examine ethical dilemmas and guidelines related to actions and decisions of individuals and organizations who create and use computer systems.

The scope of the term "computer ethics" varies considerably. Some people include such issues as the universal-access issue discussed in Section 9.2, the environmental impact of computers, the impact of computers on employment, whether to sell computers to totalitarian governments, and use of computers by the military. These are all important issues that involve computers, but one's opinions about them usually have more to do with one's political and social views than with one's knowledge or experience as a computer professional. I believe that "computer ethics" is more usefully defined more narrowly as a category of professional ethics, similar to medical, legal, and accounting ethics, for example. 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.

Thus, for our discussion, computer ethics includes ethical issues faced by a computer professional as part of the job. It includes relationships with and responsibilities toward customers, clients, colleagues, employers, employees, others who use and/or produce, and others whom they affect. We also include issues faced by people who are not computer professionals, but who manage, select, or use computers in a professional setting.

We look at situations where ethical decisions must be made, situations where significant consequences for you and others could result from your decisions. For example, what if your company is about to deliver a computer system to a customer and you believe it will be a serious bug? What if your supervisor asks you to make unauthorized copies of copyrighted software? Is it right to hire foreign programmers who work at low salaries? What if you are assigned to a job for a client whose business you find objectionable?

1 Donald Glaser, Personal and argued this same position in a number of computer ethic articles. It seems to be gaining acceptance among scholars i
Suppose a private company asks you to develop a database of information obtained from government records, perhaps to generate lists of convicted child molestors, perhaps marketing lists of new home buyers, affluent box 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 task? You could accept on the grounds that the records are already public and available to anyone; you could decide against secondary uses of information that was not provided voluntarily by the people it concerns; you could try to determine whether the benefits of the lists outweigh the privacy invasions or inconveniences they might cause to some people; you could refuse to make marketing lists, but agree to make lists of people convicted of certain crimes, using Pomer's principle (see Section 2.6.3) that negative information, such as convictions, should be in the public domain. The ethical first step, however, is recognizing that you face an ethical issue.

Suppose you are a manager and discover that many of your employees are spending a lot of time visiting sports, movie, and entertainment Web sites while at work. Will you install monitoring software that records what sites each employee visits and how much time he or she spends there? Will you inform employees first? Are you confusing practical and legal issues—and ethical ones?

Decisions a business or organization makes about what information to collect from visitors to its Web site and how to use that information have an ethical component. So, too, does the decision to distribute software to convert from formats with built-in copy protection to formats that can be copied more easily. 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; thus many of the ethical issues are, also.

There are special aspects to making ethical decisions in a professional context, but the decisions are fundamentally based on general ethical principles and theories. In the next section, we introduce several ethical theories. We discuss some distinctions (e.g., between ethics and law) that are important to understand when tackling ethical issues.

In Section 10.2, we return to computer technology and consider ethical guidelines for computer professionals. In Section 10.3, we consider some sample cases.

10.1.2 WHAT IS ETHICS, ANYWAY?

Ethics is the study of what is meant to "do the right thing." It is a complex subject that has occupied philosophers for thousands of years. This presentation is necessarily simplified.

Ethical theory is based on the assumption that people are rational and make free choices. Neither of these conditions is always and absolutely true. People are emotionally...
and they make mistakes. A person is not making a free choice when someone else is pointing a gun at him. Some argue that a person is not making a free choice in a situation where she might lose a job. However, free choice and use of rational judgment are capacities and characteristics of human beings, and they are reasonably assumed in the basis of ethical theory. We take the view that the individual is, in most circumstances, responsible for his or her actions.

Ethical rules are rules to follow in our interactions with other people and in our actions that affect other people. Most ethical theorist attempt to achieve the same goal: to enhance human dignity, peace, happiness, and well-being. Ethical rules apply to all of us and are intended to achieve good results for people in general, and for situations in general—not just for ourselves, not just the one situation. A set of rules that does this will respect the fact that we are each unique and have our own values and goals, that we have judgments and will, and that we act according to our judgment to achieve our goals. The rules should clarify our obligations and responsibilities—and our areas of choice and personal preference. (Not all ethical theories fit this description. Ethical relativism and some types of ethical egoism do not. This chapter, however, stipulates these goals and requirements for ethical theories.)

We could view ethical rules as fundamental and universal, like laws of science, or we could view them as rules we make up, like the rules of baseball, to provide a framework in which to interact with other people in a peaceful, productive way. The titles of two books illustrate these different viewpoints. One is Ethics: Discovering Right and Wrong; the other is Ethics: Inventing Right and Wrong. We do not have to decide which view is correct to find good ethical rules. In either case, our tools include reason, introspection, and observation of human nature, values, and behavior.

Behaving ethically, in a personal or professional sphere, is usually not a burden. Most of the time we are honest, we keep our promises, we do not steal, we do our jobs. This should not be surprising. Ethical rules are good ones. They work for people; that is, they make our lives better. Behaving ethically is often practical. Honesty makes interactions among people more smoothly and reliably, for example. We might lose friends if we often lie or break promises. Also, social institutions encourage us to do right. We might be scared if caught stealing. We might lose our jobs if we do them carelessly. In a professional context, doing good ethically often corresponds closely with doing a good job in the sense of professional quality and competence. Doing good ethically often corresponds closely with good business in the sense that ethically developed products are more likely to please consumers. Sometimes, however, it is difficult to do the right thing.

It takes courage in situations where we could suffer negative consequences. Courage is often associated with heroic acts, where one risks one's life to save someone in a dangerous situation—the kind of act that makes front-page news. Most of us do not have those opportunities to display courage, but we do have many opportunities in day-to-day life. 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.
10.1.3 A VARIETY OF ETHICAL VIEWS

Although there is much agreement about general ethical rules, there are many different theories about how to establish a firm justification for the rules and how to decide what is ethical in specific cases. In this section, we give brief descriptions of a few approaches to ethics. Some ethicists make a distinction between ethical theories that view certain acts as good or bad because of some intrinsic aspect of the action and ethical theories that view acts as good or bad because of their consequences. They call these deontological (for nonconsequentialist) and consequentialist theories, respectively. The distinction is perhaps emphasized more than necessary. If the criteria used by deontologists to determine the intrinsic goodness or badness of an act did not consider its consequences for people—at least for most people, most of the time—the criteria would seem to have little ethical merit.

DEONTOLOGICAL THEORIES

Deontologists tend to emphasize duty and absolute rules, to be followed whether they lead to good or ill consequences in particular cases. One example is: Do not lie. An act is ethical if it complies with ethical rules and is chosen for that reason.

Immanuel Kant, the philosopher often presented as the prime example of a deontologist, contributed many important ideas to ethical theory. We mention three of them here. One is the principle of universality: We should follow rules of behavior that we can universally apply to everyone. This principle is so fundamental to ethical theory that we already accepted it in our explanation of ethics in Section 10.1.2. The Biblical instruction, "Do unto others as you would have them do unto you," is another statement of the same general idea.

Deontologists argue that logic or reason determines rules of ethical behavior, that actions are intrinsically good because they follow from logic. Kant believed that rationality is the standard of what is good. We can reason about what makes sense and act accordingly, or we can act irrationally, which is evil. The view that something is evil because it is illogical might seem unconvincing, but Kant's instruction to "Respect the reason in you," that is, to use your reason, rationality, and judgment, rather than emotions, when making a decision in an ethical context, is a wise one.

Third, Kant stated a principle about interacting with other people: One must never use people as merely means to ends, but rather as ends in themselves.

Kant took an extreme position on the absolutism of ethical rules. He argued, for example, that it is always wrong to lie; for example, if a person is looking for someone he intends to murder, and he asks you where the intended victim is, it is wrong for you to lie to protect the victim. Most people would agree that these are cases in which even very good, universal rules should be broken—because of the consequences.

*Ethics is a philosophy (and others) who study ethics.*
UTILITARIANISM

Utilitarianism is the main example of a consequentialist theory, its guiding principle, as expressed by John Stuart Mill, is to increase happiness, or "utility." A person's utility is what satisfies the person's needs and values. An action might decrease utility for some people and increase it for others. We should consider the consequences—the benefits and damages to all affected people—and "calculate" the change in aggregate utility. An act is right if it tends to increase aggregate utility and wrong if it tends to decrease it.

Utilitarianism is a very influential theory, and it has many variations. As stated above, the utilitarian principle applies to individual actions. For each action, we consider the impact on utility and judge the action by its net impact. This is sometimes called "act utilitarianism." One variant of utilitarianism, called "rule utilitarianism," applies the utility principle not to individual actions but to general ethical rules. Thus, a rule-utilitarian might argue that the rule "Do not lie" will increase total utility, and so that reason is a good rule. Rule-utilitarians do not do a utility calculation for each instance where lying is considered. Generally, a utilitarian would be more comfortable than a deontologist breaking a rule in circumstances where doing so would have good consequences.

There are numerous problems with act-utilitarianism. It might be difficult or impossible to determine all the consequences of an act. If we can do so, do we increase what we believe will or should contribute to the happiness of the people affected, or what they choose themselves? How do we know what they would choose? How do we quantify happiness in order to make comparisons among many people? Should some people's utility be given more weight than others? Should we weigh a thief's gain of utility equal to the victim's loss? Is a dollar worth the same to a person who worked for it and a person who received it as a gift? Or to a rich person and a poor person? How can we measure the utility of freedom?

A more fundamental (and ethical) objection to act-utilitarianism is that it does not recognize or respect individual rights. It has no absolute prohibitions and so could allow actions that many people consider always wrong. For example, if there is a convincing case that killing one innocent person (perhaps to distribute his or her organs to other community members) would maximize utility in a community, utilitarianism could justify this act. A person has no protected domain of freedom. Recognizing that widespread killing and stealing decrease the security and happiness of all, a rule utilitarian can derive rules against these acts. We can state these particular rules in terms of rights to life and property.

NATURAL RIGHTS

Suppose we wish to treat people as ends rather than merely means and we wish to increase people's happiness. These goals are somewhat vague and open to many interpretations in specific circumstances. One approach we might follow is to let people make their own decisions, to define a sphere of freedom in which people can act freely according to their
own judgments, without coercive interference by others, even others (including us) who think they are doing what is best for the people involved, or for humanity in general. This approach views ethical behavior as acting in such a way that respects a set of fundamental rights of others, including the rights to life, liberty, and property. These rights are sometimes called natural rights because, in the opinion of some philosophers, they come from nature, or can be derived from the nature of humanity. We each have an exclusive right to ourselves and our labor, and to what we produce with our labor. John Locke argued for a natural right to property that we create or obtain by mixing our labor with it. Respect for these rights implies ethical rules against killing, stealing, and deception.

Those who emphasize natural rights tend to emphasize the ethical character of the powers by which people interact, seeing acts generally as likely to be ethical if they involve voluntary interaction and freely made exchanges, where the parties are not coerced or deceived. This contrasts with other approaches that tend to focus on the result or state achieved by the interaction, for example, seeing an action as likely to be unethical if it leaves some people poor.

NO SIMPLE ANSWERS

We cannot solve ethical problems by applying a formula or an algorithm. Human behavior and real human situations are complex. There are often trade-offs to consider. Ethical theories do not provide clear, unambiguously correct answers on most issues. We can use the approaches described to support opposite sides of many an issue. For example, consider Kant's imperative that one must never treat people as merely means to ends, but rather as ends in themselves. We could argue that an employee who receives a very low wage, say, a wage too low to support a family, is wrongly being treated as merely a means for the employer to make money. But we could also argue that expecting the employer to pay more than he or she considers reasonable is treating the employer merely as a means to providing income for the employer. Similarly, it is easy for two utilitarians to come to different conclusions on a particular issue by measuring happiness or utility differently. A very small set of basic natural rights might provide no guidance for many situations in which you must make ethical decisions—but, if we try to define rights to cover more situations, there will be fierce disagreement about just what those rights should be. (Recall the controversies in Chapter 2 about whether there is a right to privacy, and, if so, how far it goes.)

Although ethical theories do not completely settle difficult, controversial issues, they help to identify important principles or guidelines. They remind us of things to consider, and they can help clarify reasoning and values. There is much merit in Kant's principle of universalism and his emphasis on treating people as intrinsically valuable "ends." In utilitarianism's consideration of consequences and as a standard of increasing achievement of people's happiness, and in the natural-right approach of setting minimal rules in a rights framework to guarantee people a sphere in which they can act according to their own values and judgment.
10.1.4 SOME IMPORTANT DISTINCTIONS

A number of important distinctions affect our ethical judgments, but are often not clearly expressed or understood. In this section, we identify a few of these. Just being aware of them can help clarify issues in some ethical debates.

RIGHT, WRONG, AND OKAY

In situations with ethical dilemmas, there are often many options that are ethically acceptable, with no specific one ethically required. Thus, it is misleading to divide all acts into two categories, ethically right and ethically wrong. Rather, it is better to think of acts as ethically obligatory, ethically prohibited, or ethically acceptable.

NEGATIVE AND POSITIVE RIGHTS, OR LIBERTIES AND CLAIM-RIGHTS

In Section 10.2.2, we described two quite different kinds of rights. Recall that negative rights, or liberties, are rights to act without coercive interference. Claim-rights, or positive rights, are rights that impose an obligation on some people to provide certain things for others. We have seen that the distinction is important in debates about privacy, fair use of intellectual property, universal access to the Web, and other issues in this book. It is important in analyzing ethical scenarios, too.

DISTINGUISHING WRONG AND HARM

Carelessly and needlessly causing harm is wrong, but it is important to remember that harm alone is not a sufficient criterion to determine that an act is unethical. Many ethical, even admirable, acts can make other people worse off. For example, you may accept a job offer knowing someone else wanted the job and needed it more than you do. You may reduce the income of other programmers by writing a better program that consumers prefer. If your program is really good, you may put a competitive out of business completely and cause many people to lose their jobs. Yet there is nothing wrong with doing honest, productive work.

On the other hand, hackers argue that breaking into computer systems without authorization is not wrong because they do no harm. Lack of harm is not sufficient to conclude that an act is ethically acceptable. Aside from the fact that the hacker might do unintended harm, one can argue that hacking is a violation of property rights: A person has no right to enter your property without your permission, independent of any harm done.

SEPARATING GOAL FROM CONSTRAINTS

Economist Milton Friedman has written that the goal or responsibility of a business is to make a profit for its shareholders. This statement appealed some ethicists, as they believe it justifies, or is used to justify, irresponsible and unethical actions. It seems to me that arguments on this point miss the distinction between goals on the one hand, and constraints on actions that may be taken to achieve the goals, on the other— or the
distinction between ends and means. Our personal goals may include financial success and finding an attractive mate. Working hard, investing wisely, and being an interesting and decent person can achieve these goals. They may be achievable as well by stealing and lying. By most ethical theories, stealing and lying are unacceptable. Ethics tells us what actions are acceptable or unacceptable in our attempt to achieve the goals. There is nothing unethical about a business having the goal of maximizing profits. The ethical character of the company depends on whether the actions taken to achieve the goal are consistent with ethical constraints.

PERSONAL PREFERENCE AND ETHICS

There are many issues about which we have strong feelings, some related to our ethical views. It might be difficult to draw a line between what we consider ethically wrong and what we personally disapprove of. Pick an organization that advocates some policy you deeply think is ethically wrong, perhaps an abortion rights group or an anti-abortion group, or a group that advocates legalizing marriages between same-sex couples, or a group that advocates banning homosexuals from teaching in public schools. Suppose the group is solely an advocacy or educational group; it does not perform abortions or block abortion clinics, for example. Now, the organization asks you, a programmer, to write a software package, perhaps a mailing-list program. You believe in freedom of speech, but you find the job distasteful; you do not want to do anything to assist the organization.

If you decide to decline the job, are you acting on ethical grounds? In other words, can you claim that performing the job is unethical? The organization is encroaching freedom of speech. Although its position is controversial and ethical issues are relevant to the social issue the organization supports, the organization is not engaged in unethical activity. Your assistance would help to further a goal you do not support. This is a matter of personal preference. There is nothing ethically wrong with declining the assignment, of course; the consumer’s freedom of speech does not impose an ethical obligation on you for assistance.

When discussing political or social issues, people frequently argue that their position is right in a moral or ethical sense or that an opponent’s position is morally wrong or unethical. People tend to want to be on the “moral high ground” and feel the stigma of an accusation that their view is ethically wrong. Thus, arguments based on ethics can be, and often are, used to intimidate people with different views. It is a good idea to try to distinguish between actions we find distasteful, rude, or ill-advised and actions that we can argue convincingly are ethically wrong.

LAW AND ETHICS

What is the connection between law and ethics? Very little. Is it ethical to prohibit marijuana use by terminally ill people? Is it ethical for the government or a state university to give preference in contracts, hiring, or admissions to people in specific ethnic groups? Is it ethical to sell mailing lists based on customer purchasing history? Whatever the current law happens to be does not answer these questions. In addition, history provides
numerous examples of laws most of us consider profoundly wrong by ethical standards; slavery is perhaps the most obvious example. Ethics precedes law in the sense that ethical principles help determine whether or not we should pass specific laws.

Some laws enforce ethical rules (e.g., against murder and theft). By definition, we are ethically obligated to obey such laws—not because they are laws, but because the laws implement the obligations and prohibitions of ethical rules.

Other laws fall into several categories, we look at the ethical character of a few of them. One category of laws establishes conventions for business or other activities. Commercial law, such as the Uniform Commercial Code, defines rules for economic transactions and contracts. Such rules provide a framework in which we can interact smoothly and confidently with strangers. They include provisions for how to interpret a contract if a court must resolve a dispute. These laws are extremely important to any society. They should be consistent with ethics; beyond basic ethical considerations, however, details could depend on historic conventions, practicality, and other nonethical criteria. In the U.S., drivers must drive on the right side of the road; in England, drivers must drive on the left side. There is obviously nothing intrinsically right or wrong about either choice, but, once the convention is established, it is ethically wrong to drive on the wrong side of the road because it endangers other people.

Unfortunately, many laws fall into a category that is not intended to implement ethical rules—or even be consistent with them. The political process is subject to pressure from special interest groups of all sorts who seek to pass laws that favor their groups or businesses. Examples include the laws that delayed the introduction of cable television (promoted by the television networks) and laws, sponsored by the dairy industry when margarine was first introduced, against coloring margarine yellow to look more like butter. Many prominent people in the financial industry reported receiving a large number of fund-raising letters from members of Congress—in the week that Congress took up new regulations for their industry. Many political, religious, or ideological organizations promote laws to require (or prohibit) certain kinds of behavior that the group considers desirable (or objectionable). Examples include prohibitions on gambling or alcohol, requirements for recycling, and requirements that stores close on Sundays. At an extreme, in some countries, this category includes restrictions on the practice of certain religions.

Copyright law has elements of all three categories we described. It defines a property right, violation of which is a form of theft. Because of the intangible nature of intellectual property, some of the rules about what constitutes infringement are more like the second category: pragmatic rules that are devised to be workable. Powerful groups (e.g., the publishing, music, and movie industries) lobby for specific rules to benefit themselves. This is why some violations of copyright law are clearly unethical (if one accepts the concept of intellectual property at all), yet others seem to be entirely acceptable, sometimes even noble.

Are we ethically obligated to obey a law just because it is a law? Some argue that we are. As members of society, we are obligated to accept the rules that are made by the legislative process so long as they are not clearly and utterly ethically wrong (e.g., slavery).
10.2 Ethical Guidelines for Computer Professionals

In this section, we look at problems and characteristics of professional ethics, as distinct from general ethics. We look at guidelines developed by scholars and computer professionals, including the Software Engineering Code of Ethics and Professional Practice and the ACM Code of Ethics and Professional Conduct (included in Appendix A).

10.2.1 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. 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 problems of many professionals (e.g., 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 security 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; many 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, competent professionals have special responsibilities not only to their customers, but also to the general public.
DO ORGANIZATIONS HAVE ETHICS?

This is a relevant question here because we will be discussing decisions made in a professional context. Computer software and systems are not usually produced by one individual alone. They are produced by a company or organization, and the decisions about design, testing, and so on, are made within an organizational structure.

Some philosophers argue that it is meaningless to speak of an organization as having ethics. Individual people make all decisions and take all actions; these people must have ethical responsibility for everything they do. Others argue that an organization that acts with intention and a formal decision structure, such as a business, is a moral entity. Viewing a business as a moral entity does not diminish the responsibility of the individual people. Ultimately, it is individuals who are making decisions and taking actions. We can hold both the individuals and the company or organization responsible for their acts.*

Whether one accepts or rejects the idea that a business can have moral rights and responsibilities, it is clear that organizational structure and policies lead to a pattern of actions and decisions that have ethical content. Businesses do have a "corporate culture," or a "personality," or simply a reputation for treating employees and customers in respectful or ungrateful or careless and deceptive—ways. A bug in a new checkout-scanner program developed for Walgreens, a drugstore chain, occasionally caused an incorrect price to be charged. Walgreens delayed introduction of a new inventory control system for six months while they solved the problem. The same person working at a different company might have made the opposite decision. The policies and principles of the company influence such decisions. People in management positions shape the corporate culture or ethics of the business. Thus, decisions by managers have an impact beyond the particular product or contract the decision involves. A manager who is dishonest with customers or who cuts corners on testing, for example, is setting an example that encourages other employees to be dishonest and careless. A manager's ethical responsibility includes his or her contribution to the company's ethical personality. Principle 5 of the Software Engineering Code of Ethics and Professional Practice includes many specific guidelines for managers.

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 4, 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 is enormously complex, and the

---

* Some philosophers argue that it is meaningless to speak of an organization as having ethics. Individual people make all decisions and take all actions; these people must have ethical responsibility for everything they do. Others argue that an organization that acts with intention and a formal decision structure, such as a business, is a moral entity. Viewing a business as a moral entity does not diminish the responsibility of the individual people. Ultimately, it is individuals who are making decisions and taking actions. We can hold both the individuals and the company or organization responsible for their acts. Whether one accepts or rejects the idea that a business can have moral rights and responsibilities, it is clear that organizational structure and policies lead to a pattern of actions and decisions that have ethical content. Businesses do have a "corporate culture," or a "personality," or simply a reputation for treating employees and customers in respectful or ungrateful or careless and deceptive—ways. A bug in a new checkout-scanner program developed for Walgreens, a drugstore chain, occasionally caused an incorrect price to be charged. Walgreens delayed introduction of a new inventory control system for six months while they solved the problem. The same person working at a different company might have made the opposite decision. The policies and principles of the company influence such decisions. People in management positions shape the corporate culture or ethics of the business. Thus, decisions by managers have an impact beyond the particular product or contract the decision involves. A manager who is dishonest with customers or who cuts corners on testing, for example, is setting an example that encourages other employees to be dishonest and careless. A manager's ethical responsibility includes his or her contribution to the company's ethical personality. Principle 5 of the Software Engineering Code of Ethics and Professional Practice includes many specific guidelines for managers.
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 also 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 engaging a sophisticated computer system includes knowing or learning enough about the system to avoid creating potential problems.

10.2.2 PROFESSIONAL CODES, GUIDELINES, AND RESPONSIBILITIES

PROFESSIONAL CODES OF ETHICS

Many professional organizations have codes of professional conduct. They provide a general statement of ethical values that members in the profession accept as ethical behavior expected of them. The codes are designed specifically to address 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 training experience may not have prepared them to be alert to difficult ethical situations and handle them appropriately.

There are several organizations for the range of professions included in the general term "computer professionals." The main ones are the ACM and the IEEE Computer Society (IEEE CS). 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 the cases in Section 10.3, 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, to maintain professional competence, to 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 to computer systems. They

*The organizations mentioned in this code are the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers.

1SE Code, 1.0. 2.0. 6.0 2.0. 7.0 3.0. ACM Code 1.1. 1.1
2SE Code, 2.0. ACM Code 1.2
3SE Code 8.0. ACM Code 2.2
4SE Code 8.0. ACM Code 2.4
5ACM Code 2.6
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 Software Engineering Code covers many specific points about software development. It was translated into several languages and adopted by various organizations as their internal professional standard.

SOME GUIDELINES

We highlight a few principles for producing good systems. Most are directed at software developers. 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.

Understand what success means. After the utter fiasco of opening day at Kaua‘i Lii`a’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. No role was to get passengers, crews, planes, baggage, 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.

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 4.1.4 and 4.3.2), where confusing user interfaces and system behavior increased the risk of accidents. There are numerous “human errors” of systems developed by technical people without sufficient knowledge of what was important to users. For example, a system developed for a newborn nursery at a hospital rounded each baby’s weight to the nearest pound; for premature babies, the difference in a few ounces is crucial. The responsibility of developers to talk to users is not restricted to systems that affect safety and health. A system designed to process stories in a newspaper office, to manage inventory in a toy store, or to manage a personal computer’s desktop could cause frustration, might waste a chemist’s money, and might be discarded if designed without sufficient consideration of the needs of actual 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.)

---

1 SE Code 1.09, 3.12; ACM Code: 1.7
2 SE Code 1.03; ACM Code: 1.2
3 SE Code 2.02, 2.03; ACM Code: 1.5, 1.6, 2.8
WHAT SHOULD NOT BE IN A PROFESSIONAL CODE?

Professional codes of ethics are usually written by dedicated people with the goal of guiding practitioners in the field and protecting the public; it would never be overlooked. The recommendations are sometimes included for the purpose of guiding could serve the interests of professional members of the profession rather than all practitioners and the public. For example, the discussion of laws on telemedicine practice by out-of-state doctors under Section 9.2.2.

Would opposition to competition affect a decision to select or endorse a product in a professional code? The medical organizations used a temporary hold on a leading manufacturer's drug in negotiating with a state legislature about a Coalition for Health Care.

Professional organizations often lobby government representatives about pay and other laws. Deals might be made that include provisions that the professional code or standards. Ethical or professional reasons. Mandated disclosures and conflicts-of-interest concerns can influence the position taken in a code. When the professional code often has the effect of reducing the number of people who belong to it, (those who are self-taught), thereby raising the image of their goals. Many in the computing profession who advocate technology, for example, the desire to improve quality of the profession and are profitable, and not to themselves incompetent practitioners.

Professional associations tend to be large: the ACM with 40,000 members. On the other hand, professional organizations are often considered to be the positions of elected individuals. The membership distribution suggests that the profession has a diversity of opinions or members of the profession, but within the dermatology, dermatology, and so to endeavor in other professions. For example, to adopt a position on a political issue of the profession would be dishonest. For example, it would seem inappropriate for an ethical code of a professional organization of computer professionals to take a position on, say, mandating high-voltage military weaponry. It is reasonable that an organization such as the Computer Professionals for Social Responsibility members of the profession to work to improve the societal and political viewpoints, would adopt positions or ethical concerns that might be appropriate for the ACM or the IEEE CS.

Design for real work. We have seen several cases where computer crashes because someone typed input incorrectly. In one case, an entire pager was given the wrong because a technician did not press the "Enter" key or did not let it load enough. Real people make typos, get confused, or are new to 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 computer users to detect all incorrect inputs, but there are techniques for catching many and for reducing the damage that errors cause.

Don't assume existing software is safe. 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 would be necessary to 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 4 that a complex 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 Asarco 5.)

Be open and honest about capabilities, safety, and limitations of software. This is important in general, and especially for expert systems or decision systems—systems that use models and heuristics incorporating expert knowledge to guide decision making—for medical diagnosis or investment planning, for example. Developers must explain the limitations and uncertainties to users (doctors, financial advisors, and so forth), and users must not shirk responsibility for understanding them and using the systems properly.

In several cases, described in Chapter 4, 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 side 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.

Regret 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. In 1986, burning gases that leaked from a rocket shortly after launch destroyed the space shuttle Challenger killing the seven people aboard.4 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 engineers 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.

4 The comment system was not at fault.

5 The comment system was not at fault.
REINFORCING EXCLUSION

A voice-recognition system is a system consisting of hardware and software that identifies the person speaking. (This is different from speech recognition, discussed in section 9.1.2, which identifies the words spoken.) One application of voice recognition is teleconferencing for business meetings, where the computer identifies who is speaking and displays that person on everyone's screen. Some voice-recognition systems can recognize male voices much more easily than female voices. For example, one system fails to recognize female speakers and displays the name of the person speaking, regardless of gender. This can lead to unfair treatment, especially if there are no alternatives to voice recognition.

Did the designer of this system envision such a problem when designing the voice-recognition system? Probably not. Are users aware of differences between males and females in the accuracy of voice-recognition systems? Probably not. What happened? These voice-recognition systems were designed by men and tested by men, primarily in meetings. Men were the primary developers and testers of these systems, and they were likely the primary users of these systems. In his book *The Road Ahead*, Bill Gates tells us that when voice-recognition systems were first developed and tested, a handshaking-recognition system was also being worked on. When it didn't work, they dropped it to focus on text-to-speech systems. Gates is right-handed, but the voice-recognition systems were developed and tested by left-handed engineers.

In some applications, it is safer to use voice-recognition systems, but the system should be designed for universality. The example Gates provides is one in which a voice-recognition system is being developed for use by the deaf. The system would need to work for people of all ages and gender, as well as those with and without disabilities. The system would also need to work for people who are left-handed or right-handed.

In these cases, using "yes" or "right" as a voice command would increase the incidence of error, especially for people who are left-handed or right-handed. The system would need to be designed to accommodate all users and expanding its potential market.

10.3 Cases

10.3.1 INTRODUCTION AND METHODOLOGY

The cases presented here are just a few samples of the kinds that can 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 of clients, the employer, coworkers, and others. Many more cases 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 fictitious scenarios, for some of these cases I give conclusions. You might face cases like those 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.

How shall we analyze specific scenarios? We now have a number of tools. We can try to apply any 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 any agreements 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 Software Engineering Code of Ethics and Professional Practice, 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, our discussions of the cases will usually include most of these elements:

1. **Brainstorming phase**
   - List rules, issues, problems, consequences.
   - List all the people and organizations affected. (They are generally referred to as the stakeholders.)
   - In cases where there is not a 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.)
   - Consider the impact of the action options on the stakeholders. Analyze consequences, risks, benefits, harms, costs for each action considered.
   - Find sections of the Software Engineering Code or the ACM Code that apply. Consider the guidelines in Sections 10.2.2. 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 values of each, courtesy to others, prudently, self-interest, personal preferences, and so on. (In some cases, there is a sequence of actions depending on the response to each.)

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

10.3.2 COPYING AN EMPLOYEE’S FILES

You are a computer system manager. An employee is out sick and another employee requests that you copy all files from the sick person’s computer so he or she can do some work.

One risk here is invasion of privacy; the sick employee might have personal files stored on the computer. Also, the sick employee could have files related to secret or proprietary company information to which other employees are not supposed to have access. There is a small risk to you and the company from a complaint or suit for invasion of privacy if you copy personal files. On the other hand, the employee making the request and the company might suffer if important work is not completed on time.

The obvious stakeholders include the sick employee, the employee making the request, and you (the system manager). There are others. Other people working on the same project might suffer negative consequences if lack of access to needed files delays its completion. Your action could set a precedent affecting privacy of the files of all employees who use the computers you manage. In any business scenario, if the revenue and success of the business as a whole could be seriously affected, the owners (perhaps thousands of stockholders) and other employees are stakeholders. In this case, we will assume the impact on this group is minor.

There might be a very simple solution to this problem. Call the sick employee, and ask permission to copy the files. But be or be she not be reachable. Another option would be to request authorization from the manager of the project on which the employee is working.

The right thing to do depends in large part on the policies, practices, and expectations at the particular company. If there is a strong policy against personal use of the computer system, then it is routine practice for employees to share files while working on a project, and if it is reasonable to believe that all the files to be copied are related to the project the employees are working on, there might be no ethical problem with copying the files.

(Note: SE Code 5.03.) In the actual case, the system manager refused to transfer all the
10.3.3 INSUFFICIENT PRIVACY PROTECTION

Your customer is a community clinic that works with families that have problems of family violence. The clinic has three sites in the same city, including a shelter for battered women and children. Currently, the clinic uses no computers. 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 in-office communication for e-mail communication with other social-service agencies about client needs. She owns a few notebook computers capable of storing copies of records that staffs carry when they visit clients at home. At the shelter, staffs use only first names, but the records contain last names and forwarding addresses of women who have recently left. The director's description of the system makes no mention of passwords or encryption. 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 is less likely to be aware of the risks of a computer system. You, as the computer professional, have specialized knowledge in this area. It is in your interest to help the director of the clinic as it is in 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 3.13.2.)

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

Suppose you warn the director about unauthorized access to sensitive information by staff members and crackers and the potential for interception of records and e-mail transmitted without encryption. You suggest a list of measures to protect client privacy including, for example, a unique user ID and password for each staff member. To allow access only to information that the particular worker needs, an audit-trail function that keeps track of who accessed and modified the records, an ID code system (not Social Security number) that can be used when discussing clients with other agencies that do not need their names, and encryption for transmission of records. (Note that your ability to provide appropriate suggestions is dependent on your professional competence in security.) You tell the director that carrying records on notebook computers...
his time of unanticipated leakage, both accidental and via a bribe to a staff member. (Suppose a donor is a candidate for the city council or a party in a child-custody case.) You suggest procedures to reduce such lapses. 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 extra cost, your professional ethical behavior has helped improve the security of the system and protect client privacy.

What if the director says she cannot afford the additional features and is willing to have the system developed without them? You have several options. You can develop the cheaper, but more vulnerable, system. You can refuse and perhaps lose the job (although your refusal may 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 features 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 cases where only the customer would take the risk, none would say yes; it is your job to inform, not more. Others would say that the customer lacks the professional expertise to evaluate the risks. In this scenario, however, the decision is not the only priority at risk, but 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 more difficult decision may be deciding what is acceptable. 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, good judgment, and perhaps on consulting others who develop systems for similar applications (see Code 7.08)*.

10.3.4 Risky Systems

*Note that although this code suggests the need for prudence concerning how to spend the money, it does not suggest that you have a professional ethical responsibility to insist that the system be developed without the additional features. The code does not suggest that you have a professional ethical responsibility to insist that the system be developed with the additional features; it only suggests that you should consider the risk to clients from exposure of sensitive information.
The central issue here is safety. Your company is building a machine that is designed to save lives, but if it malfunctions, it can kill or injure patients.Perhaps the situation seems obvious: Delivering the machine 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 (the stakeholders)? First, the patients to be treated with the machine. A malfunction could cause injury or death. On the other hand, if the release of the machine is delayed, some patients might have to wait for urgent surgery instead. We will assume treatment with the laser 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 if the laser is not used. Second, the hospitals and clinics who will purchase the machine are affected. Delay could cause financial losses if they have planned on having the machine at a particular time. However, it is reasonable for them to expect that the machine has been professionally designed and fully tested. You are deceiving the customers if you do not tell them that testing was not completed. Third, your decision affects you and your company (including its shareholders and employees). 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 is delivered and 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 could have both negative and positive impacts on the managers 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, for 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 aside of longer-term risks.

Now that we have seen that arguments can be made 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 such real-world events as operating input and control of machinery. We assume that the original test plan for the last machine was directed for good reasons. The tests should be completed before delivery. (See SE Code 1.03 and 3.10 and ACM Code 1.2.)

Some patients will benefit from on-time delivery. Should they be weighed equally against the patients whose malfunction may fatal? 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 health of people who rely on existing treatments. Your machine is being offered as an improvement. 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 this 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 judgments in a way that does not exploit people, without their knowledge, for additional harm.*

What about your responsibility to your company? Even if we weigh the short-term effects of one delay more highly than the risks of losses that would result from a malfunction, the ethical arguments are on the side of deferring 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 20.1.4.) Perhaps the distinction would be more obvious if the same were true for 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 1.62).

16.3.5 GOING PUBLIC

Suppose you are a member of a team working on a computer-controlled catheter ablation system for automobiles. You think the system has a flaw that could endanger people. The project manager does not seem concerned and expects no evidence of completion of the project soon. Are you ethically obligated to do something?

Given the potential consequences, yes (see SE Code 1.94, ACM Code 1.2, 2.9). We consider a variety of options. First, as a minimum, discuss your concerns with the project manager. Misusing your concerns is admirable and obligatory. It is also good for your company's 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 evaluation of the problem, your next option is to go to someone higher up in the company.

* They are many situations where patients knowingly rely on existing treatments. Here, we are guessing the danger device is not being decided to rely on experimental but at most, presently safe, treatment device.
If no one with authority in the company is willing to investigate your concerns you may 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 if negative publicity kills the project altogether. 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 risk is real, or if you are aware of a careless, irresponsible attitude among the company management, then you are obligated to go further (see Code 6.15). You are not an involved bystander, for whom the question of ethical obligation may be more fuzzy. The project pays your salary. You are part of the team; you are a participant. (Note that this is the kind of situation suggested in the Software Engineering Code, Section 2.05, where you may violate a confidentiality agreement.)

There have been several dramatic cases where professionals faced this difficult situation. The engineers who worked on the rockets for the space shuttle Challenger knew that it was not safe to launch the shuttle in cold weather. They argued for a delay and tried to convince their managers and NASA officials of the danger. When the decision was made to approve the launch, the engineers faced the issue we are confronting here. Should they have done more, perhaps gone to others in their company or NASA, or to the news media, to stop the launch? In another example, computer engineers who worked on the San Francisco Bay Area Rapid Transit system (BART) were concerned 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 that changes were needed. Eventually, one of their critical memos and reports were published in a newspaper. The engineers were fired. During the next few years, while several crashes occurred, there were public investigations and numerous recommendations made for improving safety of the system.12

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.13

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.
18.3.6 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 medical clinic, or a large credit bureau. Someone asks you to get a copy of a personal file. He will pay you $500.

Where is the stakeholder? You! You have an opportunity to make some extra money. The person seeking the file: Presumably he has something to gain from it. The person whose file is requested: His or her privacy will be violated. All people about whose company or agency has personal files: If you sell one file, chances are you will sell others if asked in the future. Your employer (at a private company): If the sale becomes known, the victim might sue the company; if such sales of files 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 file. Refuse. Say nothing about the incident. Report the incident to your supervisor. Report it to the police. Contact the person whose file was requested and tell him or her of the incident. Agree to sell the file, 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 file, is wrong. It almost certainly violates rules and policies you have agreed to abide by in accepting your job. As an employee, you are bound by the guarantees of confidentiality the company or agency has promised its customers or the public. Depending on how the information in the file is to be used, you could be helping to cause serious harm to the victim. (See ACM Code: 1.2, 1.3, 1.7, 2.6; SE Code: 2.03, 2.05, 2.09, 4.04, 4.05.)

Some would argue that selling the file 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 file, you might not be under an ethical obligation to keep it secret. The essential difference that makes selling the file wrong in this scenario is your position of trust as an employee in a company or agency that maintains sensitive files.

None of the other actions we listed are ethically required. They are all ethically required. Depending on policies of the employer and laws related to certain government agencies (see SE Code 2.06 and ACM Code 2.33), you might be obligated to report any attempts 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 serve as a useful lesson to someone who wishes to commit such a crime.

Some ethicists, e.g., theologians, argue that taking an action because it benefits you is not ethically misconduct. 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 required to do more than refuse
to sell the file. It is difficult to decide how much you are obligated to do to prevent a
wrong thing from happening if you are not participating in the wrong act. A thief
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 files 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 (perhaps anonymously), 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 are not directly involved;
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 not be disclosed. In this case, you know that sensitive
information is being sold. Thus the argument in favor of an obligation to take action is
stronger (see SF Code 6.13 and 7.01).

10.3.7 CONFLICT OF INTEREST

You have a small consulting business. The CyberStuff company plans to acquire a
new Web-site hosting system and it wants to hire you to evaluate bids from vendors.
Your spouse works for NetWorks and did most of the work in writing the bid that
NetWorks 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 NetWorks?

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

I have seen two immediate reactions to scenarios similar to the one (in discussions
among professionals and among students). One is that it is a simple case of profit 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 benefitting from the contract or disclosing
your connection and losing the contract?
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 on a field site next to the company office.

Where 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 very certain, 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. Tackling these address issues such as: Will the device withstand heat, water, and snow? 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?

The New York City Fire Commissioner halted use of a $35 million digital communications system after a firefighter's call for help on his radio was not heard. Firefighters...
10.3.9 COPYRIGHT VIOLATION

Your company has about 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 are caught? There are several possible actions. Give up, you did your best to correct the problem. Call the software vendor or the Software and Information Industry Association 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 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. As a practical matter, your name on the license could expose you to legal risk or to being made a scapegoat by unethical managers in your company. 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 signs the licenses, then you observed a wrong being done 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 SEC Code and 1.5 and 2.6 of the ACM Code suggest?

10.3.10 HIRING FOREIGN PROGRAMMERS

You are a manager at a software company about to begin a large software project. You will need to hire dozens of new programmers. Using the Internet for communication and software delivery, you can hire programmers in another country at lower salary than programmers in your country. Should you do this?13

This case differs from others we considered in that it involves wider social and economic issues. I include it for several reasons. It is a real, current controversy. Hiring of foreign programmers who work in their home country has been increasing, with potentially significant implications for the economies and the programmers in the countries involved. This is a good example for trying to discern economic advantage from ethical arguments. We explicitly consider Kantian and utilitarian approaches in the analysis. Also, in other industries, several countries have passed legislation to restrict the hiring of foreign workers. The discussion here might provide insight into the ethics of such legislation. For simplicity, I use the U.S. as the country where the software company is
based. U.S. companies hire programmers in India, Russia, and elsewhere. I use India in the
discussion.

The people most obviously affected by the decision in this case are the Indian pro-
grammers and the U.S. programmers you might hire. Before we consider other stake-
holders, we will use utilitarianism and Kant's principle about treating people as ends in
themselves to generate some ideas, questions, and observations about these two groups.
How can we compare the impact on utility from the two choices? The number of people
hired will be about the same in either case. There does not appear to be any reason,
from an ethical point of view, for placing a higher weight on the utility of one group
of programmers merely because of their nationality. Shall we weigh the utilities of the
programmers according to the number of dollars they will receive? That favors hiring
the U.S. programmers. Or should we weigh utility by comparing the pay to the average
salary in each country? That favors hiring the Indians. The today obtained from a
job for an individual programmer depends on the availability of other jobs. Are there
more opportunities to earn a comparable income in the U.S. or in India? We see that a
calculation of net utility for the programmers depends on how one evaluates the utility
of the jobs for each group of programmers.

What happens when we apply Kant's principle? When we hire people for a job, we
are interacting with them in a limited role. We are making a trade, money for work. The
programmers are a means to an end: producing a marketable product is a reasonable
price. Kant does not say that people must not be treated as a means to an end, but
rather that they should not be treated merely as such. Kant does not seem helpful here,
especially if we observe that the hiring decision does not treat the potential programmers
differently in a way that has to do with ends and means.

Are you taking advantage of the Indian programmers, perhaps "exploiting" them
by paying them less than you would have to pay the U.S. programmers? Some people
believe it is unfair to both the U.S. and Indian programmers that the Indians get the jobs
by charging less money. It is equally logical, however, to argue that paying the lower
rate for U.S. programmers is wasteful, or charity, or simply overlap. What makes
either pay level more "right" than the other? Buyers would like to pay less for what they
buy, and sellers would like to get a higher price for their goods and services. There is
nothing automatically unethical about choosing the cheaper of two products, services, or
employment.

We can argue that treating the Indian programmers as ends in themselves includes
respecting the choices and trade-offs they make to better their lives according to their
own judgment, in particular in offering to work for lower wages than U.S. programmers,
because there are special cases in which we might decide otherwise. First, suppose your
company is using something to limit the other options of the Indian programmers. If
your company is lobbying for import restrictions on software produced by Indian firms,
for example, thus decreasing the availability of other programming jobs in India, then
you are manipulating the programmers into a situation where they have few or no other
choices. In that case, you are not respecting their freedom and allowing them to compete
Clearly, you are, then, not treating them as ends in themselves. We will assume for the rest of the discussion that your company is not doing anything like this.

Another reason we might decide that the Indian programmers are not being treated as ends in themselves, or with respect for their human dignity, is that their working conditions would be worse than the working conditions expected by U.S. workers (or required by law in the U.S.). The programmers might not get medical insurance. They might work in rundown, crowded offices, lacking air-conditioning. Is hiring them to work in such conditions unethical, or does it give them an opportunity to improve conditions in their country? Whether or not it is ethically required, there are several reasons why you might pay more (or provide better working conditions) than market conditions in India require: a sense of shared humanity that motivates you to want to provide conditions you consider desirable, a sense of generosity (i.e., willingness to contribute to the improvement of the standard of living of people in a country less rich than your own) and economic benefits: paying more than expected may get you a high morale, productivity, and company loyalty.

Many laws have been passed to require that the same salary be paid to all workers when a large group of potential workers (foreigners, ethnic minorities, low-skilled workers, teenagers) is willing to work for lower pay. The main argument is that such laws will prevent the less-advantaged workers from being exploited. Historically, one of the effects of these laws is that the traditionally higher-paid group gets most of the jobs. (Often this has been the intent of the law.) In this case, the almost certain result would be that the U.S. programmers would be hired. The law, or an ethical requirement that the Indian programmers be paid the same as the U.S. programmers, would protect the high incomes of programmers in the U.S. and the profits of companies that pay higher salaries. New workers or businesses that are trying to compete by lowering prices generally oppose such requirements.

So far, we have been discussing the impact of your decision on the programmers only. Other people are affected, too: your customers, the owners or stockholders of your company, and, indirectly, and to a smaller degree, many people in other businesses. Hiring the Indian programmers increases the utility of your company and customers. The customers benefit from the lower price of the product, and the owners of the company benefit from the profits. If the product is successful, the company might pay for advertising, distribution, and so on, providing jobs for others in the United States. On the other hand, if you hire U.S. programmers, they will spend more of their earnings in the U.S. than the Indian programmers, generating jobs and income for others. If the product is not profitable because of higher programming costs, the company could go out of business, with a negative impact on all its employees and suppliers. To which of all these people do you have responsibilities or obligations? As a manager of the company, you have an obligation to help sell the product and make the company successful; to manage the project so that it maximizes profit (not in a manner independent of ethical considerations, as we have noted, but in one consistent with them). Unless the owners of the company have a policy to improve the standard of living of people in other countries or to "buy American," your obligation to them includes hiring competitive workers at the best price. You have
some responsibility for the fate of other company employees who might lose their jobs
if you do a poor job of managing the project. You do not have any special obligation
to other service providers you could hire, nor to people seeking jobs as programmers
in other countries.

Although hiring cheaper workers in other countries is often described as ethically
suspect, this discussion suggests that there is no strong ethical argument for that view.

EXERCISES

Review Exercises

30.1 What are two of Kant’s important ideas about ethics?
30.2 What is the difference between act-utilitarianism and rule-utilitarianism?
30.3 Give an example of a law that implements an ethical principle. Give an example of a law that
efforts to a particular group’s desires about how people should behave.
30.4 What are two ways professional ethics differ from ethics in general?

General Exercises

10.5 Give an argument in support of “Do not lie” as a moral general ethical rule. Identify which of your
arguments are utilitarian and which are deontological.
10.6 Which kind of ethical theory, deontological or consequentialist, works better for arguing that it is
wrong to drive on the left side of a road in a country where people normally drive on the
right? Explain.
10.7 Describe a case at work or in school where you were asked or pressured to do something you
thought unethical.
10.8 A computer science professor in a computer-security class assigned students to break into a com-
puter system and bring back specific files to prove that they had. The owner of the system was
unaware of the assignment. Analyze this case from an ethical perspective, using the methodology
of Section 10.3.1. Consider both the ethics of the professor in making this assignment and your
response as a student in the class. Are there non-computer analogies that can help in the analysis?

In Section 2.5.1, we mentioned an incident in which a woman who filled out a detailed customer-
profile questionnaire received an offensive and demeaning letter from a travel agent. Her
inmates had been hired to enter the questionnaire data into a computer database. What are
the ethical issues involved in a direct-mailing company’s decision about whether to contract with
a prison system or use a more expensive commercial data-entry service? In hindsight, we know
that the incident in this case had various negative consequences. Do you think the company
should have foreseen such a problem, or was the decision one of the key factors in the data-entry task
a reasonable one?

10.10 Review the description of the airplane crash near Columbia in Section 4.3.2. Find specific
guidelines in Sections 10.2.2 and the ethics codes in Appendix 4.1 that, if followed carefully, might
have avoided problems in the flight-management software that contributed to the crash.