E

ETHICS AND PROFESSIONAL RESPONSIBILITY IN COMPUTING

INTRODUCTION

Computing professionals perform a variety of tasks: They write specifications for new computer systems, they design instruction pipelines for superscalar processors, they diagnose timing anomalies in embedded systems, they test and validate software systems, they restructure the back-end databases of inventory systems, they analyze packet traffic in local area networks, and they recommend security policies for medical information systems. Computing professionals are obligated to perform these tasks conscientiously because their decisions affect the performance and functionality of computer systems, which in turn affect the welfare of the systems' users directly and that of other people less directly. For example, the software that controls the automatic transmission of an automobile should minimize gasoline consumption and, more important, ensure the safety of the driver, any passengers, other drivers, and pedestrians.

The obligations of computing professionals are similar to the obligations of other technical professionals, such as civil engineers. Taken together, these professional obligations are called *professional ethics*. Ethical obligations have been studied by philosophers and have been articulated by religious leaders for many years. Within the discipline of philosophy, ethics encompasses the study of the actions that a responsible individual should choose, the values that an honorable individual should espouse, and the character that a virtuous individual should have. For example, everyone should be honest, fair, kind, civil, respectful, and trustworthy. Besides these general obligations that everyone shares, professionals have additional obligations that originate from the responsibilities of their professional work and their relationships with clients, employers, other professionals, and the public.

The ethical obligations of computing professionals go beyond complying with laws or regulations; laws often lag behind advances in technology. For example, before the passage of the Electronic Communications Privacy Act of 1986 in the United States, government officials did not require a search warrant to collect personal information transmitted over computer communication networks. Nevertheless, even in the absence of a privacy law before 1986, computing professionals should have been aware of the obligation to protect the privacy of personal information.

WHAT IS A PROFESSION?

Computing professionals include hardware designers, software engineers, database administrators, system analysts, and computer scientists. In what ways do these occupations resemble recognized professions such as medicine, law, engineering, counseling, and accounting? In what ways do computing professions resemble occupations that are not thought of traditionally as professions, such as plumbers, fashion models, and sales clerks?

Professions that exhibit certain characteristics are called *strongty differentiated* professions (1). These professions include physicians and lawyers, who have special rights and responsibilities. The defining characteristics of a strongly differentiated profession are specialized knowledge and skills, systematic research, professional autonomy, a robust professional association, and a well-defined social good associated with the profession.

Members of a strongly differentiated profession have specialized knowledge and skills, often called a "body of knowledge," gained through formal education and practical experience. Although plumbers also have special knowledge and skills, education in the trades such as plumbing emphasizes apprenticeship training rather than formal education. An educational program in a professional school teaches students the theoretical basis of a profession, which is difficult to learn without formal education. A professional school also socializes students to the values and practices of the profession. Engineering schools teach students to value efficiency and to reject shoddy work. Medical schools teach students to become physicians, and law schools teach future attorneys. Because professional work has a significant intellectual component, entry into a profession often requires a post-baccalaureate degree such as the M.S.W. (Master of Social Work) or the Psy.D. (Doctor of Psychology).

Professionals value the expansion of knowledge through systematic research; they do not rely exclusively on the transmission of craft traditions from one generation to the next. Research in a profession is conducted by academic members of the professioin and sometimes by practitioner members too- Academic physicians, for example, conduct medical research. Because professionals understand that professional knowledge always advances, professionals should also engage in continuing education by reading publications and attending conferences. Professionals should share general knowledge of their fields, rather than keeping secrets of a guild. Professionals are obligated, however, to keep specific information about clients confidential.

Professionals tend to have *clients*, not *customers*. Whereas a sales clerk should try to satisfy the customer's *desires*, the professional should try to meet the client's *needs* (consistent with the welfare of the client and the public). For example, a physician should not give a patient a prescription for barbiturates just because the patient wants the drugs but only if the patient's medical condition warrants the prescription.

Because professionals have specialized knowledge, clients cannot fully evaluate the quality of services provided by professionals. Only other members of a profession, the

Wiley Encyclopedia of Computer Science and Engineering, edited by Benjamin Wah.

professional's peers, can sufficiently determine the quality of professional work. The principle of peer review underlies accreditation and licensing activities: Members of a profession evaluate the quality of an educational program for accreditation, and they set the requirements for the licensing of individuals. For example, in the United States, a lawyer must pass a state's bar examination to be licensed to practice in that state. (Most states have reciprocity arrangements—a professional license granted by one state is recognized by other states.) The license gives professionals legal authority and privileges that are not available to unlicensed individuals. For example, a licensed physician may legitimately prescribe medications and perform surgery, which are activities that should not be performed by people who are not medical professionals.

Through accreditation and licensing, the public cedes control over a profession to members of the profession. In return for this autonomy, the profession promises to serve the public good. Medicine is devoted to advancing human health, law to the pursuit of justice, and engineering to the economical construction of safe and useful objects. As an example of promoting the public good over the pursuit of self-interest, professionals are expected to provide services to some indigent clients without charge. For instance, physicians volunteer at free clinics, and they serve in humanitarian missions to developing countries. Physicians and nurses are expected to render assistance in cases of medical emergency—for instance, when a train passenger suffers a heart attack. In sum, medical professionals have special obligations that those who are not medical professionals do not have.

The purposes and values of a profession, including its commitment to a public good, are expressed by its code of ethics. A fortiori, the creation of a code of ethics is one mark of the transformation of an occupation into a profession.

A profession's code of ethics is developed and updated by a national or international professional association. This association publishes periodicals and hosts conferences to enable professionals to continue their learning and to network with other members of the profession. The association typically organizes the accreditation of educational programs and the licensing of individual professionals.

Do computing professions measure up to these criteria for a strongly differentiated profession? To become a computing professional, an individual must acquire specialized knowledge about discrete algorithms and relational database theory and specialized skills such as software development techniques and digital system design. Computing professionals usually learn this knowledge and acquire these skills by earning a baccalaureate degree in computer science, computer engineering, information systems, or a related field. As in engineering, a bachelor's degree currently suffices for entry into the computing professions. The knowledge base for computing expands through research in computer science conducted in universities and in industrial and government laboratories.

Like electrical engineers, most computing professionals work for employers, who might not be the professionals' clients. For example, a software engineer might develop application software that controls a kitchen appliance; the engineer's employer might be different from the appliance manufacturer. Furthermore, the software engineer should prevent harm to the ultimate users of the appliance and to others who might be affected by the appliance. Thus, the computing professional's relationship with a client and with the public might be indirect.

The obligations of computing professionals to clients, employers, and the public are expressed in several codes of ethics. The later section on codes of ethics reviews two codes that apply to computing professionals.

Although the computing professions meet many criteria of other professions, they are deficient in significant ways. Unlike academic programs in engineering, relatively few academic programs in computing are accredited. Furthermore, in the United States, computing professionals cannot be licensed, except that software engineers can be licensed in Texas. As of this writing, the Association for Computing Machinery (ACM) has reaffirmed its opposition to state-sponsored licensing of individuals (2). Computing professionals may earn proprietary certifications offered by corporations such as Cisco, Novell, Sun, and Microsoft. In the United States, the American Medical Association dominates the medical profession, and the American Bar Association dominates the legal profession, but no single organization defines the computing profession. Instead, multiple distinct organizations exist, including the ACM, the Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS), and the Association of Information Technology Professionals (AIPT). Although these organizations cooperate on some projects, they remain largely distinct, with separate publications and codes of ethics.

Regardless of whether computing professions are strongly differentiated, computing professionals have important ethical obligations, as explained in the remainder of this article.

WHAT IS MORAL RESPONSIBILITY IN COMPUTING?

In the early 1980s Atomic Energy of Canada Limited (AECL) manufactured and sold a cancer radiation treatment machine called the Therac 25, which relied on computer software to control its operation. Between 1985 and 1987, the Therac-25 caused the deaths of three patients and serious injuries to three others (3). Who was responsible for the accidents? The operator who administered the massive radiation overdoses, which produced severe burns? The software developers who wrote and tested the control software, which contained several serious errors? The system engineers who neglected to install the backup hardware safety mechanisms that had been used in previous versions of the machine? The manufacturer, AECL? Government agencies? We can use the Therac-25 case to distinguish among four different kinds of responsibility (4,5).

Causal Responsibility

Responsibility can be attributed to causes: For example, "the tornado was responsible for damaging the house." In the Therac-25 case, the proximate cause of each accident was the operator, who started the radiation treatment. But just as the weather cannot be blamed for a moral failing, the

Therac-25 operators cannot be blamed because they followed standard procedures, and the information displayed on the computer monitors was cryptic and misleading.

Role Responsibility

An individual who is assigned a task or function is considered the responsible person for that role. In this sense, a foreman in a chemical plant may be responsible for disposing of drums of toxic waste, even if a forklift operator actually transfers the drums from the plant to the truck. In the Therac-25 case, the software developers and system engineers were assigned the responsibility of designing the software and hardware of the machine. Insofar as their designs were deficient, they were responsible for those deficiencies because of their roles. Even if they had completed their assigned tasks, however, their role responsibility may not encompass the full extent of their professional responsibilities.

Legal Responsibility

An individual or an organization can be legally responsible, or liable, for a problem. That is, the individual could be charged with a crime, or the organization could be liable for damages in a civil lawsuit. Similarly, a physician can be sued for malpractice. In the Therac-25 case, AECL could have been sued. One kind of legal responsibility is *strict liability*: If a product injures someone, then the manufacturer of the product can be found liable for damages in a lawsuit, even if the product met all applicable safety standards and the manufacturer did nothing wrong. The principle of strict liability encourages manufacturers to be careful, and it provides a way to compensate victims of accidents.

Moral Responsibility

Causal, role, and legal responsibilities tend to be exclusive: If one individual is responsible, then another is not. In contrast, moral responsibility tends to be shared: many engineers are responsible for the safety of the products that they design, not just a designated safety engineer. Furthermore, rather than assign blame for a past event, moral responsibility focuses on what individuals should do in the future. In the moral sense, responsibility is a virtue: A "responsible person" is careful, considerate, and trustworthy; an "irresponsible person" is reckless, inconsiderate, and untrustworthy.

Responsibility is shared whenever multiple individuals collaborate as a group, such as a software development team. When moral responsibility is shared, responsibility is *not* atomized to the point at which no one in the group is responsible. Rather, each member of the group is accountable to the other members of the group and to those whom the group's work might affect, both for the individual's own actions and for the effects of their collective effort. For example, suppose a computer network monitoring team has made mistakes in a complicated statistical analysis of network traffic data, and that these mistakes have changed the interpretation of the reported results. If the team members do not reanalyze the data themselves, they have an obligation to seek the assistance of a statistician who can analyze the data correctly. Different team members might work with the statistician in different ways, but they should hold each other accountable for their individual roles in correcting the mistakes. Finally, the team has a collective moral responsibility to inform readers of the team's initial report about the mistakes and the correction.

Moral responsibility for recklessness and negligence is not mitigated by the presence of good intentions or by the absence of bad consequences. Suppose a software tester neglects to sufficiently test a new module for a telephone switching system, and the module fails. Although the subsequent telephone service outages are not intended, the software tester is morally responsible for the harms caused by the outages. Suppose a hacker installs a keystroke logging program in a deliberate attempt to steal passwords at a public computer. Even if the program fails to work, the hacker is still morally responsible for attempting to invade the privacy of users.

An individual can be held morally responsible both for acting and for failing to act. For example, a hardware engineer might notice a design flaw that could result in a severe electrical shock to someone who opens a personal computer system unit to replace a memory chip. Even if the engineer is not specifically assigned to check the electrical safety of the system unit, the engineer is morally responsible for calling attention to the design flaw, and the engineer can be held accountable for failing to act.

Computing systems often obscure accountability (5). In particular, in an embedded system such as the Therac-25, the computer that controls the device is hidden. Computer users seem resigned to accepting defects in computers and software that cause intermittent crashes and losses of data. Errors in code are called "bugs," regardless of whether they are minor deficiencies or major mistakes that could cause fatalities. In addition, because computers seem to act autonomously, people tend to blame the computers themselves for failing, instead of the professionals who designed, programmed, and deployed the computers.

WHAT ARE THE RESPONSIBILITIES OF COMPUTING PROFESSIONALS?

Responsibilities to Clients and Users

Whether a computing professional works as a consultant to an individual or as an employee in a large organization, the professional is obligated to perform assigned tasks competently, according to professional standards. These professional standards include not only attention to technical excellence but also concern for the social effects of computers on operators, users, and the public. When assessing the capabilities and risks of computer systems, the professional must be candid: The professional must report all relevant findings honestly and accurately. When designing a new computer system, the professional must consider not only the specifications of the client but also how the system might affect the quality of life of users and others. For example, a computing professional who designs an information system for a hospital and should allow speedy access

by physicians and nurses and yet protect patients' medical records from unauthorized access; the technical requirement to provide fast access may conflict with the social obligation to ensure patients' privacy.

Computing professionals enjoy considerable freedom in deciding how to meet the specifications of a computer system. Provided that they meet the minimum performance requirements for speed, reliability, and functionality, within an overall budget, they may choose to invest resources to decrease the response time rather than to enhance a graphical user interface, or vice versa. Because choices involve tradeoffs between competing values, computing professionals should identify potential biases in their design choices (6). For example, the designer of a search engine for an online retailer might choose to display the most expensive items first. This choice might favor the interest of the retailer, to maximize profit, over the interest of the customer, to minimize cost.

Even moderately large software artifacts (computer programs) are inherently complex and error-prone. Furthermore, software is generally becoming more complex. It is therefore reasonable to assume that all software artifacts have errors. Even if a particular artifact does not contain errors, it is extremely difficult to prove its correctness. Faced with these realities, how can a responsible software engineer release software that is likely to fail sometime in the future? Other engineers confront the same problem, because all engineering artifacts eventually fail. Whereas most engineering artifacts fail because physical objects wear out, software artifacts are most likely to fail because of faults *designed into* the original artifact. The intrinsically faulty nature of software distinguishes it from light bulbs and I-beams, for example, whose failures are easier to predict statistically.

To acknowledge responsibilities for the failure of software artifacts, software developers should exercise due diligence in creating software, and they should be as candid as possible about both known and unknown faults in the software—particularly software for *safety-critical systems*, in which a failure can threaten the lives of people. Candor by software developers would give software consumers a better chance to make reasonable decisions about software before they buy it (7). Following an established tradition in medicine, Miller (8) advocates "software informed consent" as a way to formalize an ethical principle that requires openness from software developers. Software informed consent requires software developers to reveal, using explanations that are understandable to their customers, the risks of their software, including the likelihoods of known faults and the probabilities that undiscovered faults still exist. The idea of software informed consent motivates candor and requires continuing research into methods of discovering software faults and measuring risk.

Responsibilities to Employers

Most computing professionals work for employers. The employment relationship is contractual: The professional promises to work for the employer in return for a salary and benefits. Professionals often have access to the employer's proprietary information such as trade secrets, and the professional must keep this information confidential. Besides trade secrets, the professional must also honor other forms of *intellectual property* owned by the employer: The professional does not have the right to profit from independent sale or use of this intellectual property, including software developed with the employer's resources.

Every employee is expected to work loyally on behalf of the employer. In particular, professionals should be aware of potential conflicts of interest, in which loyalty might be owed to other parties besides the employer. A *conflict of interest* occurs when a professional is asked to render a judgment, but the professional has personal or financial interests that may interfere with the exercise of that judgment. For instance, a computing professional may be responsible for ordering computing equipment, and an equipment vendor owned by the professional's spouse might submit a bid. In this case, others would perceive that the marriage relationship might bias the professional's judgment. Even if the spouse's equipment would be the best choice, the professional's judgment would not be trustworthy. In a typical conflict of interest situation, the professional should *recuse* herself: that is, the professional should remove herself and ask another qualified person to make the decision.

Many computing professionals have managerial duties, and some are solely managers. Managerial roles complicate the responsibilities of computing professionals because managers have administrative responsibilities and interests within their organizations in addition to their professional responsibilities to clients and the public.

Responsibilities to Other Professionals

Although everyone deserves respect from everyone else, when professionals interact with each other, they should demonstrate a kind of respect called *collegiality*. For example, when one professional uses the ideas of a second professional, the first should credit the second. In a research article, an author gives credit by properly citing the sources of ideas from other authors in previously published articles. Using these ideas without attribution constitutes plagiarism. Academics consider plagiarism unethical because it represents the theft of ideas and the misrepresentation of those ideas as the plagiarist's own.

Because clients cannot adequately evaluate the quality of professional service, individual professionals know that their work must be evaluated by other members of the same profession. This evaluation, called *peer review* occurs in both practice and research. Research in computing is presented at conferences and is published in scholarly journals. Before a manuscript that reports a research project can be accepted for a conference or published in a journal, the manuscript must be reviewed by peer researchers who are experts in the subject of the manuscript.

Because computing professionals work together, they must observe *professional standards*. These standards of practice are created by members of the profession or within organizations. For example, in software development, one standard of practice is a convention for names of variables in code. By following coding standards, a software developer can facilitate the work of a software maintainer who

subsequently modifies the code. For many important issues for which standards would be appropriate theoretically, however, "standards" in software engineering are controversial, informal, or nonexistent. An example of this problem is the difficulties encountered when the IEEE and the ACM attempted to standardize a body of knowledge for software engineering to enable the licensing of software engineers.

Senior professionals have an obligation to *mentor* junior professionals in the same field. Although professionals are highly educated, junior members of a profession require additional learning and experience to develop professional judgment. This learning is best accomplished under the tutelage of a senior professional. In engineering, to earn a P.E. license, a junior engineer must work under the supervision of a licensed engineer for at least four years. More generally, professionals should assist each other in continuing education and professional development, which are generally required for maintaining licensure.

Professionals can fulfill their obligations to contribute to the profession *volunteering*. The peer review of research publications depends heavily on volunteer reviewers and editors, and the activities of professional associations are conducted by committees of volunteers.

Responsibilities to the Public

According to engineering codes of ethics, the engineer's most important obligation is to ensure the safety, health, and welfare of the public. Although everyone must avoid endangering others, engineers have a special obligation to ensure the safety of the objects that they produce. Computing professionals share this special obligation to guarantee the safety of the public and to improve the quality of life of those who use computers and information systems.

As part of this obligation, computing professionals should enhance the public's understanding of computing. The responsibility to educate the public is a collective responsibility of the computing profession as a whole; individual professionals might fulfill this responsibility in their own ways. Examples of such public service include advising a church on the purchase of computing equipment and writing a letter to the editor of a newspaper about technical issues related to proposed legislation to regulate the Internet.

It is particularly important for computing professionals to contribute their technical knowledge to discussions about public policies regarding computing. Many communities are considering controversial measures such as the installation of Web filtering software on public access computers in libraries. Computing professionals can participate in communities' decisions by providing technical facts. Technological controversies involving the social impacts of computers are covered in a separate article of this encyclopedia.

When a technical professional's obligation of loyalty to the employer conflicts with the obligation to ensure the safety of the public, the professional may consider *whistlebhwing,* that is, alerting people outside the employer's organization to a serious, imminent threat to public safety. Computer engineers blew the whistle during the development of the Bay Area Rapid Transit (BART) system near San Francisco (9). In the early 1970s, three BART engineers became alarmed by deficiencies in the design of the electronics and software for the automatic train control system, deficiencies that could have endangered passengers on BART trains. The engineers raised their concerns within the BART organization without success. Finally, they contacted a member of the BART board of directors, who passed their concerns to Bay Area newspapers. The three engineers were immediately fired for disloyalty. They were never reinstated, even when an accident proved their concerns were valid. When the engineers sued the BART managers, the IEEE filed an *amicus curiae* brief on the engineers' behalf, stating that engineering codes of ethics required the three engineers to act to protect the safety of the public. The next section describes codes of ethics for computing professionals.

CODES OF ETHICS

For each profession, the professional's obligations to clients, employers, other professionals, and the public are stated explicitly in the profession's code of ethics or code of professional conduct. For computing professionals, such codes have been developed by ACM, the British Computer Society (BCS), the, IEEE-CS, the AITP, the Hong Kong Computer Society, the Systems Administrators Special Interest Group of USENEX (SAGE), and other associations. Two of these codes will be described briefly here: the ACM code and the Software Engineering Code jointly approved by the IEEE-CS and the ACM.

The ACM is one of the largest nonprofit scientific and educational organization devoted to computing. In 1966 and 1972, the ACM published codes of ethics for computing professionals. In 1992, the ACM adopted the current Code of Ethics and Professional Conduct (10), which appears in Appendix 1. Each statement of the code is accompanied by interpretive guidelines. For example, the guideline for statement 1.8, *Honor confidentiality*, indicates that other ethical imperatives such as complying with a law may take precedence. Unlike ethics codes for other professions, one section of the ACM code states the ethical obligations of "organizational leaders," who are typically technical managers.

The ACM collaborated with the IEEE-CS to produce the Software Engineering Code of Ethics and Professional Practice (11). Like the ACM code, the Software Engineering Code also includes the obligations of technical managers. This code is notable in part because it was the first code to focus exclusively on software engineers, not on other computing professionals. This code is broken into a short version is composed of and a long version. The short version is composed of a preamble and eight short principles; this version appears in Appendix 2. The long version expands on the eight principles with multiple clauses that apply the principles to specific issues and situations.

Any code of ethics is necessarily incomplete—no document can address every possible situation. In addition, a code must be written in general language; each statement in a code requires interpretation to be applied in specific circumstances. Nevertheless, a code of ethics can serve

multiple purposes (12,13). A code can inspire members of a profession to strive for the profession's ideals. A code can educate new members about their professional obligations, and tell nonmembers what they may expect members to do, A code can set standards of conduct for professionals and provide a basis for expelling members who violate these standards. Finally, a code may support individuals in making difficult decisions. For example, because all engineering codes of ethics prioritize the safety and welfare of the public, an engineer can object to unsafe practices not merely as a matter of individual conscience but also with the full support of the consensus of the profession. The application of a code of ethics for making decisions is highlighted in the next section.

ETHICAL DECISION MAKING FOR COMPUTING PROFESSIONALS

Every user of e-mail has received unsolicited bulk commercial e-mail messages, known in a general way as *spam*. (A precise definition of "spam" has proven elusive and is controversial; most people know spam when they see it, but legally and ethically a universally accepted definition has not yet emerged.) A single spam broadcast can initiate millions of messages. Senders of spam claim that they are exercising their free speech rights, and few laws have been attempted to restrict it. In the United States, no federal law prohibited spamming before the CAN-SPAM Act of 2003. Even now, the CAN-SPAM law does not apply to spam messages that originate in other countries. Although some prosecutions have occurred using the CAN-SPAM Act, most people still receive many e-mail messages that they consider spam.

Some spam messages are designed to be deceptive and include intentionally inaccurate information, but others include only accurate information. Although most spamming is not illegal, even honest spamming is considered unethical by many people, for the following reasons. First, spamming has bad consequences: It wastes the time of recipients who must delete junk e-mail messages, and these messages waste space on computers; in addition, spamming reduces users' trust in e-mail. Second, spamming is not reversible: Senders of spam do not want to receive spam. Third, spamming could not be allowed as a general practice: If everyone attempted to broadcast spam messages to wide audiences, computer networks would become clogged with unwanted e-mail messages, and no one could communicate via e-mail at all.

The three reasons advanced against spam correspond to three ways in which the morality of an action can be evaluated: first, whether on balance the action results in more good consequences than bad consequences; second, whether the actor would be willing to trade places with someone affected by the action: and third, whether everyone (in a similar situation) could choose the same action as a general rule. These three kinds of moral reasons correspond to three of the many traditions in philosophical ethics: consequentialism, the Golden Rule, and duty-based ethics.

Ethical issues in the use of computers can also be evaluated through the use of analogies to more familiar situations. For example, a hacker may try to justify gaining unauthorized access to unsecured data by reasoning that because the data are not protected, anyone should be able to read it. But by analogy, someone who finds the front door of a house unlocked is not justified in entering the house and snooping around. Entering an unlocked house is trespassing, and trespassing violates the privacy of the house's occupants.

When making ethical decisions, computing professionals can rely not only on general moral reasoning but also on specific guidance from codes of ethics, such as the ACM Code of Ethics (10). Here is a fictional example of that approach.

Scenario: XYZ Corporation plans to monitor secretly the Web pages visited by its employees, using a data mining program to analyze the access records. Chris, an engineer at XYZ, recommends that XYZ purchase a data mining program from Robin, an independent contractor, without mentioning that Robin is Chris's domestic partner. Robin had developed this program while previously employed at UVW Corporation, without the awareness of anyone at UVW.

Analysis: First, the monitoring of Web accesses intrudes on employees' privacy; it is analogous to eavesdropping on telephone calls. Professionals should respect the privacy of individuals (ACM Code 1.7, *Respect the privacy of others*, and 3.5, *Articulate and support policies that protect the dignity of users and others affected by a computing system).* Second, Chris has a conflict of interest because the sale would benefit Chris's domestic partner. By failing to mention this relationship, Chris was disingenuous (ACM Code 1.3, *Be honest and trustworthy).* Third, because Robin developed the program while working at UVW, some and perhaps all of the property rights belong to UVW. Robin probably signed an agreement that software developed while employed at UVW belongs to UVW. Professionals should honor property rights and contacts (ACM Code 1.5, *Honor property rights including copyrights and patent*, and 2.6, *Honor contracts, agreements, and assigned responsibilities).*

Applying a code of ethics might not yield a clear solution of an ethical problem because different principles in a code might conflict. For instance, the principles of honesty and confidentiality conflict when a professional who is questioned about the technical details of the employer's forthcoming product must choose between answering the question completely and keeping the information secret. Consequently, more sophisticated methods have been developed for solving ethical problems. Maner (14) has studied and collected what he calls "procedural ethics, step-by-step ethical reasoning procedures ... that may prove useful to computing professionals engaged in ethical decision-making." Maner's list includes a method specialized for business ethics (15), a paramedic method (16), and a procedure from the U.S. Department of Defense (17). These procedures appeal to the problem-solving ethos of

engineering, and they help professionals avoid specific traps that might otherwise impair a professional's ethical judgment. No procedural ethics method should be interpreted as allowing complete objectivity or providing a mechanical algorithm for reaching a conclusion about an ethical problem, however, because all professional ethics issues of any complexity require subtle and subjective judgments.

COMPUTING AND THE STUDY OF ETHICS: THE ETHICAL CHALLENGES OF ARTIFICIAL INTELLIGENCE AND AUTONOMOUS AGENTS

Many ethical issues, such as conflict of interest, are common to different professions. In computing and engineering, however, unique ethical issues develop from the creation of machines whose outward behaviors resemble human behaviors that we consider "intelligent." As machines become more versatile and sophisticated, and as they increasingly take on tasks that were once assigned only to humans, computing professionals and engineers must rethink their relationship to the artifacts they design, develop, and then deploy.

For many years, ethical challenges have been part of discussions of artificial intelligence. Indeed, two classic references in the field are by Norbert Wiener in 1965 (18) and by Joseph Weizenbaum in 1976 (19). Since the 1990s, the emergence of sophisticated "autonomous agents," including Web "bots" and physical robots, has intensified the ethical debate. Two fundamental issues are of immediate concern: the responsibility of computing professionals who create these sophisticated machines, and the notion that the machines themselves will, if they have not already done so, become sufficiently sophisticated so that they will be considered themselves moral agents, capable of ethical praise or blame independent of the engineers and scientists who developed them. This area of ethics is controversial and actively researched. A full discussion of even some of the nuances is beyond the scope of this article. Recent essays by Floridi and Sanders (20) and Himma (21) are two examples of influential ideas in the area.

APPENDIX 1. ACM CODE OF ETHICS AND PROFESSIONAL CONDUCT

http://www.acm.org/about/code-of-ethics.

PREAMBLE

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4.

The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the imperatives of Section 1, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.

1. GENERAL MORAL IMPERATIVES

As an ACM member I will . . ..

1.1 Contribute to society and human well-being

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.

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.

1.2 Avoid harm to others

"Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, employers. Harmful actions include

intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses."

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. See principle 2.5 regarding thorough evaluations.

1.3 Be honest and trustworthy

Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.

A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member will exercise care to not misrepresent ACM or positions and policies of ACM or any ACM units.

1.4 Be fair and take action not to discriminate

The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other such similar factors. However, these ideals do not justify unauthorized use of computer resources nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

1.5 Honor property rights including copyrights and patent

Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior. Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned

1.6 Give proper credit for intellectual property

Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.

1.7 Respect the privacy of others

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

1.8 Honor confidentiality

The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

2 MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES

As an ACM computing professional I will . . ..

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work

Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

2.2 Acquire and maintain professional competence

Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways: doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

2.3 Know and respect existing laws pertaining to professional work

ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must also be obeyed. But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

2.4 Accept and provide appropriate professional review

Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate, individual members should seek and utilize peer review as well as provide critical review of the work of others.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks

Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in imperative 1.3.

As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for imperative 1.2 for more details concerning harm, including the reporting of professional violations.

2.6 Honor contracts, agreements, and assigned responsibilities

Honoring one's commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

A computing professional has a responsibility to request a change in any assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client, should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority.

A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one's concerns and reasons for that judgment, but failing to procure a change in that assignment, one may yet be obligated, by contract or by law, to proceed as directed. The computing professional's ethical judgment should be the final guide in deciding whether or not to proceed. Regardless of the decision, one must accept the responsibility for the consequences.

However, performing assignments "against one's own judgment" does not relieve the professional of responsibility for any negative consequences.

2.7 Improve public understanding of computing and its consequences

Computing professionals have a responsibility to share technical knowledge with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing.

2.8 Access computing and communication resources only when authorized to do so

Theft or destruction of tangible and electronic property is prohibited by imperative 1.2 - "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle (see 1.4), No one should enter or use another's computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time.

3. ORGANIZATIONAL LEADERSHIP IMPERATIVES

As an ACM member and an organizational leader, I will . . ..

BACKGROUND NOTE: This section draws extensively from the draft IFIP Code of Ethics, especially its sections on organizational ethics and international concerns. The ethical obligations of organizations tend to be neglected in most codes of professional conduct, perhaps because these codes are written from the perspective of the individual member. This dilemma is addressed by stating these imperatives from the perspective of the organizational leader. In this context "leader" is viewed as any organizational member who has leadership or educational responsibilities. These imperatives generally may apply to organizations as well as their leaders. In this context "organizations" are corporations, government agencies, and other "employers," as well as volunteer professional organizations.

3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities

Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social responsibility. Therefore, organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.

3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life

Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources

Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.

3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements

Current system users, potential users and other persons whose lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.

3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system

Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems

This complements the imperative on public understanding (2.7). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge and skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems. In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

4. COMPLIANCE WITH THE CODE

As an ACM member I will ….

4.1 Uphold and promote the principles of this code

The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

4.2 Treat violations of this code as inconsistent with membership in the ACM

Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.

APPENDIX 2: SOFTWARE ENGINEERING CODE OF ETHICS AND PROFESSIONAL PRACTICE (SHORT VERSION)

http://www.acm.org/about/se-code/
Short Version

PREAMBLE

The short version of the code summarizes aspirations at a high level of the abstraction; the clauses that are included in the full version give examples and details of how these aspirations change the way we act as software engineering professionals. Without the aspirations, the details can become legalistic and tedious; without the details, the aspirations can become high sounding but empty; together, the aspirations and the details form a cohesive code.

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

1. PUBLIC - Software engineers shall act consistently with the public interest.
2. CLIENT AND EMPLOYER - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
3. PRODUCT - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. JUDGMENT - Software engineers shall maintain integrity and independence in their professional judgment.
5. MANAGEMENT - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. PROFESSION - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. COLLEAGUES - Software engineers shall be fair to and supportive of their colleagues.
8. SELF - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

BIBLIOGRAPHY

1. A. Goldman. *The Moral Foundation of Professional Ethics*, Totowa, NJ: Rowman & Littlefield, 1980.
2. J. White and B. Simons, ACM's position on the licensing of software engineers, *Communications ACM*, **45**(11): 91, 2002.
3. N. G. Leveson and C. S. Turner, An investigation of the Therac-25 accidents, *Computer*, **26**(7): 18–41, 1993.
4. J. Ladd, Collective and individual moral responsibility in engineering: some questions, *IEEE Technology and Society Magazine*, **1**(2): 3–10, 1982.
5. H. Nissenbaum, Computing and accountability, *Communications of the ACM*, **37**(1): 73–80, 1994.
6. B. Friedman and H. Nissenbaum, Bias in computer systems, *ACM Transa. Informa. Sys.*, **14**(3): 330–347, 1996.
7. C. Kaner, Blog: Software customer bill of right. Available: from http://www.satisfice.com/kaner/.
8. K. Miller, Software informed consent: docete emptorem, not caveat emptor, *Science Engineer. Ethics*, **4**(3): 357–362, 1998.
9. G. D. Friedlander, The case of the three engineers vs. BART, *IEEE Spectrum*, **11**(10): 69–76, 1974.
10. R. Anderson, D. G. Johnson, D. Gotterbarn, and J. Perrolle, Using the new ACM code of ethics in decision making, *Communications ACM*, **36**(2): 98–107, 1993.
11. D. Gotterbarn, K. Miller, and S. Rogerson, Software engineering code of ethics is approved, *Communications ACM*, **42**(10): 102–107, 1999.
12. M. Davis, Thinking like an engineer: the place of a code of ethics in the practice of a profession, *Philosophy and Public Affairs*, **20**(2): 150–167, 1991.
13. D. Gotterbarn, Computing professionals and your responsibilities: virtual information and the software engineering code of ethics, in D. Langford (ed.), *Internet Ethics*, New York: St. Martin's Press, 2000, pp. 200–219.
14. W. Maner, Heuristic methods for computer ethics, *Metaphilosophy*, **33**(3): 339–365, 2002.
15. D. L. Mathison, Teaching an ethical decision model that skips the philosophers and works for real business students, *Proceedings, National Academy of Management*, New Orleans: 1987, pp. 1–9.
16. W. R. Collins and K. Miller, A paramedic method for computing professionals, *J. Sys. Software*, **17**(1): 47–84, 1992.
17. "United States Department of Defense. Joint ethics regulation DoD 5500.7-R." 1999. Available: http://www.defenselink.mil/dodg/defense_ethics/ethics_regulation/jerl-4.doc.
18. N. Wiener, *Cybernetics: or the Control and Communication in the Animal and the Machine*, Cambridge, MA: MIT Press, 1965.

19. J. Weizenbaum, *Computer Power and Human Reason: From Judgment to Calcution*, New York: WH Freeman & Co., 1976.

20. L. Floridi and J. Sanders On the morality of artificial agents, *Minds and Machines*, **14**(3): 349–379, 2004.

21. K. Himma, There's something about Mary: the moral value of things *qua* information objects, *Ethics Informat. Technol.*, **6**(3): 145–159, 2004.

FURTHER READING

D. G. Johnson, Professional ethics, in *Computer Ethics*, 3rd ed., Upper Saddle River, NJ: Prentice Hall, 2001, pp. 54–80.

M. J. Quinn, Professional ethics, in *Ethics for the Information Age*, Boston, MA: Pearson/Addison-Wesley, 2005, pp. 365–403.

H. Tavani, Professional ethics, codes of conduct, and moral responsibility, in *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*, New York: Wiley, 2004, pp. 87–116.

MICHAEL C. LOUI
University of Illinois at Urbana-Champaign
Urbana, Illinois
KEITH W. MILLER
University of Illinois at Springfield
Springfield, Illinois