Using the New ACM CODE OF ETHICS IN Decision Making

Ronald E. Anderson
Deborah G. Johnson
Donald Gotterbarn
Judith Perrolle

Historically, professional associations have viewed codes of ethics as mechanisms to establish their status as a profession or as a means to regulate their membership and thereby convince the public that they deserve to be self-regulating. Self-regulation depends on ways to deter unethical behavior of the members, and a code, combined with an ethics review board, was seen as the solution. Codes of ethics have tended to list possible violations and threaten sanctions for such violations. ACM's first code, the Code of Professional Conduct, was adopted in 1972 and followed this model. The latest ACM code, the Code of Ethics and Professional Conduct, was adopted in 1992 and takes a new direction.

ACM and many other societies have had difficulties implementing an ethics review system and came to realize that self-regulation depends mostly on the consensus and commitment of its members to ethical behavior. Now the most important rationale for a code of ethics is an embodiment of a set of commitments of that association's members. Sometimes these commitments are expressed as rules and sometimes as ideals, but the essential social function is to clarify and formally state those ethical requirements that are important to the group as a professional association. The new ACM Code of Ethics and Professional Conduct follows this philosophy.

Recent codes of ethics emphasize socialization or education rather than enforced compliance. A code can work toward the collective good even though it may be a mere distillation of collective experience and reflection. A major benefit of an educationally oriented code is its contribution to the group by clarifying the professionals' responsibility to society.

A code of ethics holds the profession accountable to the public. This tends to yield a major payoff in terms of public trust. In Frankel's words, "To the extent that a code confers benefits on clients, it will help persuade the public that professionals are deserving of its confidence and respect, and of increased social and economic rewards" [8].

The final and most important function of a code of ethics is its role as an aid to individual decision making. In the interest of facilitating better ethical decision making, we have developed a set of nine classes that describe situations calling for ethical decision making. These cases address in turn the topics of intellectual property, privacy, confidentiality, professional quality, fairness or discrimination, liability, software risks, conflicts of interest, and unauthorized access to computer systems.

Within each case we begin with a scenario to illustrate a typical ethical decision point and then lay out the different imperatives (principles) of the new Code of Ethics that pertain to that decision. There are 24 princi-

ples in the Code and each case analysis calls on at least two or three different principles to evaluate the relevant ethical concerns. Each of the principles is relevant to at least one scenario, and some principles apply to several situations. The purpose of these case analyses is to provide examples of practical applications of the new ACM Code of Ethics.

Case 1: Intellectual Property

Jean, a statistical database programmer, is trying to write a large statistical program needed by her company. Programmers in this company are encouraged to write about their work and to publish their algorithms in professional journals. After months of tedious programming, Jean has found herself stuck on several parts of the program. Her manager, not recognizing the complexity of the problem, wants the job completed within the next few days. Not knowing how to solve the problems, Jean remembers that a coworker had given her source listings from his current work and from an early version of a commercial software package developed at another company. On studying these programs, she sees two areas of code which could be directly incorporated into her own program. She uses segments of code from both her coworker and the commercial software, but does not tell anyone or mention it in the documentation. She completes the project and turns it in a day ahead of time. (Adapted from a scenario by Dave Colantonio and Deborah Johnson.)

The Code addresses questions of intellectual property most explicitly in imperative 1.6: "Give proper credit for intellectual property . . . Specifically, one must not take credit for other's ideas or work . . ." This ethical requirement extends the property rights principle (1.5) that explicitly mentions copyrights, patents, trade secrets and license agreements. These restrictions are grounded in integrity (1.3) and in the need to comply with existing laws (2.3).

Jean violated professional ethics in two areas: failure to give credit for another's work and using code from a commercial package that presumably was copyrighted or in another

ACM CODE OF ETHICS AND PROFESSIONAL CONDUCT

On October 16, 1992, ACM's Executive Council voted to adopt a revised Code of Ethics. The following imperatives and explanatory guidelines were proposed to supplement the Code as contained in the new ACM Bylaw 17.

Commitment to ethical professional conduct is expected of every voting, associate, and student member of 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, for example with organizations such as ACM. Principles involving compliance with this Code are given in Section 4.

The Code is 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 moral imperatives section, 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. ▶

way protected by law. Suppose that Jean only looked at her coworker's source code for ideas and then completely wrote her own program; would she still have an obligation to give credit? Our answer is yes, she should have acknowledged credit to her coworker in the documentation. There is a matter of professional discretion here, because if the use of another's intellectual material is truly trivial, then there probably is no need to give formal credit.

Jean's use of commercial software code was not appropriate because she should have checked to determine whether or not her company was authorized to use the source code before using it. Even though it is generally desirable to share and exchange intellectual materials, using bootlegged software is definitely a violation of the Code.

Those interested in additional discussions on this subject should refer to the numerous articles by Pamela Samuelson on intellectual property in *Communications*. Also recommended are [2, 7, 17].

Case 2: Privacy

Three years ago Diane started her own consulting business. She has been so successful that she now has several people working for her and many clients. Their consulting work included advising on how to network microcomputers, designing database management systems, and advising about security.

Presently she is designing a database management system for the personnel office of a medium-sized company. Diane has involved the client in the design process, informing the CEO, the director of computing, and the director of personnel about the progress of the system. It is now time to make decisions about the kind and degree of security to build into the system. Diane has described several options to the client. Because the system is going to cost more than they planned, the client has decided to opt for a less secure system. She believes the information they will be storing is extremely sensitive. It will include performance evaluations, medical records for filing insurance claims, salaries, and so forth.

With weak security, employees working on microcomputers may be able to figure out ways to get access to this data, not to mention the possibilities for on-line access from hackers. Diane feels strongly that the system should be much more secure. She has tried to explain the risks, but the CEO, director of computing and director of personnel all agree that less security will do. What should she do? Should she refuse to build the system as they request? (Adapted from [14]).

In the Code of Ethics, principle number 1.7 deals with privacy and 1.8 with confidentiality. They are integrally related but the privacy principle here is the most explicit. The Guidelines of the Code say that computer professionals are obligated to preserve the integrity of data about individuals "from unauthorized access or accidental disclosure to inappropriate individuals." The Code also specifies that organizational leaders have obligations to "verify that systems are designed and implemented to protect personal privacy and enhance personal dignity" (3.5), and to assess the needs of all those affected by a system (3.4).

The company officials have an obligation to protect the privacy of their employees, and therefore should not accept inadequate security. Diane's first obligation is to attempt to educate the company officials, which is implied by imperative 2.7 to promote "public understanding of computing and its consequences." If that fails, then Diane needs to consider her contractual obligations as noted under imperative 2.6 on honoring assigned responsibilities. We do not know the details of Diane's contract, but she may have to choose between her contract and her obligation to honor privacy and confidentiality.

Additional perspectives and discussion on the privacy obligations of computer professionals can be found in [5, 6, 14, 23]. We also recommend proceedings of the latest conference on Computers, Freedom and Privacy [13].

Case 3: Confidentiality

Max works in a large state department of alcoholism and drug abuse. The agency administers programs for individuals with alcohol and drug problems, and maintains a huge database of information on the clients who use their services. Some of the data files contain the names and current addresses of clients.

Max has been asked to take a look at the track records of the treatment programs. He is to put together a report that contains the number of clients seen in each program each month for the past five years, length of each client's treatment, number of clients who return after completion of a program, criminal histories of clients, and so on. In order to put together this report, Max has been given access to all files in the agency's mainframe computer. After assembling the data into a new file that includes the client names, he downloads it to the computer in his office.

Under pressure to get the report finished by the deadline, Max decides he will have to work at home over the weekend in order to finish on time. He copies the information onto several disks and takes them home. After finishing the report he leaves the disks at home and forgets about them (adapted from [14]).

This scenario resembles the previous one that dealt with privacy considerations. However, it raises several additional issues. From the Code of Ethics, principles 1.7 on privacy and 1.8 on confidentiality apply. Imperative 2.8 on constraining access to authorized situations is also central to a computer user's decisions in this type of situation. Additionally, the Code specifies that organizational leaders have obligations to "verify that systems are designed and implemented to protect personal privacy and enhance personal dignity," (3.5) and it also states that they should specify appropriate and authorized uses of an organization's resources (3.3).

The government agency should have had policies and procedures that protected the identity of its clients. Max's relatives and friends might accidentally discover the files and inappropriately use the information to harm the reputation of the clients. The files that Max worked with for his report did not need to have any names or other information in the records that made it possible to easily identify individuals. The

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 patents

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, for example by copyright or patent.

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 ▶

agency should have removed the identifying information from the files it allowed Max to use. If that procedure had been followed, it would not have mattered that Max copied the file to his computer. Thus the organizational context created many ethical issues for Max, but unfortunately he was not attentive to these ethical issues ahead of time.

Further reading on this subject can be found in [12, 15, 20]. Discussions of computer-related procedures to maintain the confidentiality of data from specific sources also are available from other professional associations such as the American Medical Association and the American Statistical Association.

Case 4: Quality in Professional Work

A computer company is writing the first stage of a more efficient accounting system that will be used by the government. This system will save taxpayers a considerable amount of money every year. A computer professional, who is asked to design the accounting system, assigns different parts of the system to her staff. One person is responsible for developing the reports; another is responsible for the internal processing; and a third for the user interface. The manager is shown the system and agrees that it can do everything in the requirements. The system is installed, but the staff finds the interface so difficult to use that their complaints are heard by upper-level management. Because of these complaints, upper-level management will not invest any more money in the development of the new accounting system and they go back to their original, more expensive system (adapted from [10]).

The Code of Ethics advocates that computer professionals "strive to achieve the highest quality in both process and products" (2.1). Imperative 3.4 elaborates that users and those affected by a system have their needs clearly articulated.

We presume that in this case the failure to deliver a quality product is directly attributable to a failure to follow a quality process. It is likely that most of the problems with this interface would have been discovered in a review process, either with peers or with users, which is promoted by imperative 2.4. When harm results, in this case to taxpayers, the failure to implement a quality process becomes a clear violation of ethical behavior.

For recent discussions of ethics cases that deal with software quality, see [11].

Case 5: Fairness and Discrimination

In determining requirements for an information system to be used in an employment agency, the client explains that, when displaying applicants whose qualifications appear to match those required for a particular job, the names of white applicants are to be displayed ahead of those of nonwhite applicants, and names of male applicants are to be displayed ahead of those of female applicants (adapted from Donald Gotterbarn and Lionel Diemel).

According to the general moral imperative on fairness, an ACM member will be "fair and take action not to discriminate." In this case the system designer is being asked to build a system that, it appears, will be used to favor white males and discriminate against nonwhites and females. It would seem that the system designer should not simply do what he or she is told but should point out the problematic nature of what is being requested and ask the client why this is being done. Making this inquiry is consistent with 2.3 (to respect existing laws) and 2.5 (to give thorough evaluations) and 4.1 (to uphold and promote the Code of Ethics).

If the client concludes that he or she plans to use the information to favor white males, then the computer professional should refuse to build the system as proposed. To go ahead and build the system would be a violation not only of 1.4 (fairness), but of 2.3 (respecting existing laws) and would be inconsistent with 1.1 (human well-being) and 1.2 (avoiding harm).

For further discussion of the topic of bias see [9, 16, 21].

Case 6: Liability for Unreliability

A software development company has just produced a new software package that incorporates the new tax laws and figures taxes for both individuals and small businesses. The president of the company knows that the program has a number of bugs. He also believes the first firm to put this kind of software on the market is likely to capture the largest market share. The company widely advertises the program. When the company actually ships a disk, it includes a disclaimer of responsibility for errors resulting from the use of the program. The company expects it will receive a number of complaints, queries, and suggestions for modification.

The company plans to use these to make changes and eventually issue updated, improved, and debugged versions. The president argues that this is general industry policy and that anyone who buys version 1.0 of a program knows this and will take proper precautions. Because of bugs, a number of users filed incorrect tax returns and were penalized by the IRS (adapted from scenario V.7 in [18]).

The software company, the president in particular, violated several tenets of the ACM code of ethics. Since he was aware of bugs in the product, he did not strive to achieve the highest quality as called for by 2.1. In failing to inform consumers about bugs in the system, principle 2.5 was also violated.

In this instance the risks to users are great in that they have to pay penalties for mistakes in their income tax which are the result of the program. Companies by law can make disclaimers only when they are "in good conscience." The disclaimer here might not meet this legal test, in which case imperative 2.3 would be violated. As a leader in his organization the president is also violating 3.1, for he is not encouraging his staff to accept their social responsibilities.

Issues of software liability have been discussed by [19, 22].

Case 7: Software Risks

A small software company is working on an integrated inventory control system for a very large national shoe manufacturer. The system will

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 (See 1.9)

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. ▶

gather sales information daily from shoe stores nationwide. This information will be used by the accounting, shipping, and ordering departments to control all of the functions of this large corporation. The inventory functions are critical to the smooth operation of this system.

Jane, a quality assurance engineer with the software company, suspects that the inventory functions of the system are not sufficiently tested, although they have passed all their contracted tests. She is being pressured by her employers to sign off on the software. Legally she is only required to perform those tests which had been agreed to in the original contract. However, her considerable experience in software testing has led her to be concerned over risks of the system. Her employers say they will go out of business if they do not deliver the software on time. Jane contends if the inventory subsystem fails, it will significantly harm their client and its employees. If the potential failure were to threaten lives, it would be clear to Jane that she should refuse to sign off. But since the degree of threatened harm is less, Jane is faced by a difficult moral decision (adapted from [10]).

In the Code of Ethics, imperative 1.2 stresses the responsibility of the computing professional to avoid harm to others. In addition, principle 1.1 requires concern for human well-being; 1.3 mandates professional integrity, and 2.1 defines quality as an ethical responsibility. These principles may conflict with the agreements and commitments of an employee to the employer and client.

The ethical imperatives of the Code imply that Jane should not deliver a system she believes to be inferior, nor should she mislead the client about the quality of the product (1.3). She should continue to test, but she has been told that her company will go out of business if she does not sign off on the system now. At the very least the client should be informed about her reservations.

For additional discussion of software risks, [3, 22] are suggested.

Case 8: Conflicts of Interest

A software consultant is negotiating a contract with a local community to design their traffic control system. He recommends they select the TCS system out of several available systems on the market. The consultant fails to mention that he is a major stockholder of the company producing TCS software.

According to the Guidelines, imperative 2.5 means that computer professionals must "strive to be perceptive, thorough and objective when evaluating, recommending, and presenting system descriptions and alternatives." It also says that imperative 1.3 implies a computer professional must be honest about "any circumstances that might lead to conflicts of interest." Because of the special skills held by computing professionals it is their responsibility to ensure that their clients are fully aware of their options and that professional recommendations are not modified for personal gain.

Additional discussion on conflict of interest appears in [1, 25].

Case 9: Unauthorized Access

Joe is working on a project for his computer science course. The instructor has allotted a fixed amount of computer time for this project. Joe has run out of time, but he has not yet finished the project. The instructor cannot be reached. Last year Joe worked as a student programmer for the campus computer center and is quite familiar with procedures to increase time allocations to accounts. Using what he learned last year, he is able to access the master account. Then he gives himself additional time and finishes his project.

The imperative to honor property rights (1.5) has been violated. This general, moral imperative leads to imperative 2.8, which specifies that ACM members should "access communication resources only when authorized to do so." In violating 2.8 Joe also is violating the imperative to "know and respect existing laws" (2.3). As a student member of the ACM he must follow the Code of Ethics even though he may not consider himself a computing professional.

For additional reading see [4, 24,]. The most current material on this subject is likely to be found in [13].

Conclusion

These nine cases illustrate the broad range of issues a computer scientist may encounter in professional practice. While the ACM Code does not precisely prescribe what an individual must do in the situations described, it does identify some decisions as unacceptable. Often in ethical decision making many factors have to be balanced. In such situations computer professionals have to choose among conflicting principles adhering to the *spirit* of the Code as much as to the *letter*.

The ACM Code organizes ethical principles into the four categories: general moral imperatives; more specific professional responsibilities, organizational leadership imperatives, and compliance. Some may find it helpful to sort out the ethical issues involved in other ways. For example, the context of practice is relevant. Those in industry may encounter different issues from those in government or education. Those who are employed in large corporations may experience different tensions than those who work in small firms or who are self-employed. But whether working in private practice or in large organizations, computer professionals must balance responsibilities to employers, to clients, to other professionals, and to society, and these responsibilities can come into conflict. Our range of cases illustrates how one can use the general principles of the Code to deal with these diverse types of situations.

The reader may wonder why we did not have a whistle-blowing case. In a prototypical scenario, a professional has to take action which threatens the employer after concluding that the safety or well-being of some other group must take priority. Three of our cases—5, 6, 7—dealt with whistle-blowing indirectly. In all three cases, the computing professional served an outside client rather than an employer. This adds other dimensions to whistle-blowing. In Case 5, suppose the system designer learns that his client plans to use the database to discriminate and he refuses to design the system. Later he finds that a friend of his designed the system as the client wanted. He would then have to decide whether

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 computing system, software, or data files without permission. One must always have appropriate approval before using system resources, including .rm57 communication ports, file space, other system peripherals, and computer time.

3. Organizational Leadership Imperatives.

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

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 communications 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. ■

This Code and the supplemental Guidelines were developed by the Task Force for the Revision of the ACM Code of Ethics and Professional Conduct: Ronald E. Anderson, chair, Gerald Engel, Donald Gotterbarn, Grace C. Hertlein, Alex Hoffman, Bruce Jawer, Deborah G. Johnson, Doris K. Lidtke, Joyce Currie Little, Dianne Martin, Donn B. Parker, Judith A. Perrolle, and Richard S. Rosenberg. The Task Force was organized by ACM/SIGCAS and funding was provided by the ACM SIG Discretionary Fund.

to "blow the whistle" on his ex-client. These and similar types of situations are indeed important, if not common, for computer professionals. (For more prototypical situations see discussion of the Bart case and [19] on SDI.)

In all of the cases presented, we portrayed individuals acting in constrained situations. Ethical decisions depend on one's institutional context. These environments can facilitate or constrain ethical behavior. Leadership roles can set the tone and create work environments in which computer professionals can express their ethical concerns. It is significant that leadership responsibilities were demonstrated in nearly all of our nine cases. In some instances, the problem could be resolved by following the imperatives in the Code that apply to leaders. In other cases, the problem was created by a lack of ethical leadership, and the individual professional had to make a personal decision on how to proceed.

Several ethical topics were not specifically interpreted in either the Guidelines or in our cases. For instance, specific requirements of integrity for research in computing and computer science were not detailed. Nor were specific suggestions offered for maintaining professional development. These should be among the tasks of the ACM leadership to address with future additions to the Guidelines.

Other ethical issues, such as software copyright violation, were addressed but not with sufficient detail relative to their salience to the field of computing. These issues, as well as new issues not yet imagined, will confront the field of computing in the future. Not only will the Guidelines need to be updated, but there will be a need for writing and interpreting more cases typical of the ethical decisions of computing professionals. Those with special ethical computing situations are encouraged to share them with us and with others in order to foster more discussion and attention to exemplary ethical decision-making.

References

1. Bayles, M.D. *Professional Ethics.* Wadsworth, Belmont, Calif., 1981.
2. Bynum, T.W., Maner, W. and Fodor, J., Eds. *Software Ownership and Intellectual Property Rights.* Research Center on Computing and Society, Southern Connecticut State University, New Haven, Conn. 06515, 1992.
3. Clark, D. *Computers at Risk: Safe Computing in the Information Age.* National Research Council, National Academy Press, Washington, D.C., 1990.
4. Denning, P.J., Ed. *Computers under Attack: Intruders, Worms and Viruses.* Addison-Wesley, Inc., Reading, Mass., 1990.
5. Dunlop, C. and Kling, R., Eds. *Computerization and Controversy: Value Conflicts and Social Choices.* Academic Press, New York, N.Y., 1991.
6. Flaherty, D. *Protecting Privacy in Surveillance Societies.* University of North Carolina Press, Chapel Hill, N.C., 1989.
7. Forester, T. Software theft and the problem of intellectual property rights. *Comput. Soc. 20,* 1 (Mar. 1990), 2–11.
8. Frankel, M.S. Professional Codes: Why, How, and with What Impact? *J. Bus. Ethics 8* (2 and 3) (1989), 109–116.
9. Frenkel, K.A. Women and computing. *Commun. ACM 33,* 11 (Nov. 1990), 34–46.
10. Gotterbarn, D. Computer ethics: Responsibility regained. *National Forum* (Summer 1991).
11. Gotterbarn, D. Editor's corner. *J. Syst. Soft. 17* (Jan. 1992), 5–6.
12. Guynes, C.S. Protecting statistical databases: A matter of privacy. *Comput. Soc. 19,* 1 (Mar. 1989), 15–23.
13. IEEE Computer Society Press. *Proceedings of the Second Conference on Computers, Freedom and Privacy.* (Los Alamitos, Calif.), IEEE Computer Society Pres, 1992.
14. Johnson, D.G. *Computer Ethics,* Second Ed. Prentice Hall, Englewood Cliffs, N.J., 1993.
15. Laudon, K.C. *Dossier Society: Value Choices in the Design of National Information Systems.* Columbia University Press, New York, N.Y., 1986.

16. Martin, C.D. and Murche-Beyma, E., Eds. In *Search of Gender Free Paradigms for Computer Science Education.* International Society for Technology in Education, Eugene, Ore., 1992.

17. National Research Council. *Intellectual Property Issues in Software.* National Academy of Sciences, Washington, D.C., 1991.

18. Parker, D., Swope, S. and Baker, B. Ethical conflicts in information and computer science. Techology and Business. Wellesley, Mass. QED Information Sciences, 1990.

19. Parnas, D.L. SDI: A violation of professional responsibility. *Abacus 4,* 2 (Winter 1987), 46–52.

20. Perrolle, J.A. *Computers and Social Change: Information, Property, and Power.* Wadsworth, Belmont, Calif., 1987.

21. Perrolle, J. Conversations and trust in computer interfaces. In *Computers and Controversy.* Dunlop and Kling, Eds., 1991.

22. Pressman, R.S. and Herron, R. *Software Shock: The Danger and the Opportunity.* Dorsett House, 1991.

23. Salpeter, J. Are you obeying copyright law? *Technol. Learning 12,* 8 (1992), 12–23.

24. Spafford, G. Are computer hacker break-ins ethical? *J. Syst. Softw. 17* (Jan. 1992).

25. Stevenson, J.T. *Engineering Ethics: Practices and Principles.* Canadian Scholars Press, Toronto, 1987.

Note: A more extensive list of references for each of the nine specific cases, as well as general discussions of professional ethics, can be obtained by writing Ronald E. Anderson, 909 Social Sciences Bldg., University of Minnesota, Minneapolis, MN 55455. Both the ACM Code of Ethics and the bibliography are available on the Internet from acm.org using anonymous ftp or mailserve. The files are under the SIGCAS Forum and called code_of_ethics.txt and ethics_biblio.txt.