CHAPTER

1

INTRODUCTION TO CYBERETHICS: CONCEPTS, PERSPECTIVES, AND METHODOLOGICAL FRAMEWORKS

Our primary objective in Chapter 1 is to introduce some foundational concepts and methodological frameworks that will be used in our analysis of specific cyberethics issues in subsequent chapters of this textbook. To accomplish this objective, we will

- define key terms such as *cyberethics* and *cybertechnology*;
- describe key developmental phases in cybertechnology that influenced the evolution of cyberethics as a distinct field of applied ethics;
- consider whether there is anything unique or special about cyberethics issues;
- examine three distinct perspectives for identifying and approaching cyberethics issues;
- propose a comprehensive methodological scheme for analyzing cyberethics issues.

We begin by reflecting briefly on two cases, each of which illustrates a range of ethical issues that will be examined in this book.

► **CASE ILLUSTRATION I:** Verizon and the Recording Industry

In January 2003, a United States district court in the District of Columbia ruled that Verizon (an Internet Service Provider or ISP) must comply with a subpoena by the Recording Industry Association of America (RIAA)—an organization that represents the interests of the recording industry. The

RIAA, in an effort to stop the unauthorized sharing of music online, requested from Verizon the name of two of its subscribers who allegedly made available more than 600 copyrighted music files on the Internet. Although many ISPs, such as Comcast, and many universities complied with similar subpoenas issued on behalf of the RIAA, Verizon refused to release the names of any of its subscribers. Verizon argued that doing so would violate the privacy rights of its subscribers and would violate specific articles of the U.S. Constitution. So, Verizon appealed the district court's decision. On December 19, 2003, the United States Court of Appeals for the District of Columbia overturned the lower court's decision, ruling in favor of Verizon.

▶ CASE ILLUSTRATION II: The Amy Boyer Cyberstalking Case

In October 1999, twenty-year-old Amy Boyer was murdered by a young man who had stalked her via the Internet. The stalker, Liam Youens, was able to carry out most of the stalking activities that eventually led to Boyer's death by using a variety of tools available on the Internet. Using standard online search facilities available to any Internet user, Youens was able to gather personal information about Boyer. And by paying a small fee to *docusearch.com*, an online information company, Youens was able to find out where Boyer lived, where she worked, and so forth. Youens was also able to use another kind of online tool that was available to Internet users to construct two Web sites, both dedicated to his intended victim. On one site he posted personal information about Amy Boyer as well as a photograph of her. And on the other Web site Youens described, in explicit detail, his plans to murder Boyer.

First, consider the case involving Verizon and the RIAA. Here, several important ethical issues arise—concerns involving privacy and surveillance, anonymity and civil liberties, access and equity, property and ownership, and so forth. For example, consider the impact that the RIAA's actions have for a user's expectation of privacy and anonymity while navigating the Internet. Do ISPs such as Comcast and Verizon have an obligation to protect the identity of users who subscribe to their services? Should an Internet user's activities be allowed to be monitored by organizations in the private sector, such as the RIAA? Should users be able to freely exchange MP3 files that contain copyrighted music? Will allowing this practice deprive recording artists, as well as the corporations that represent them, of substantial earnings and possibly even their livelihoods? Does the unauthorized exchange of copyrighted music files over the Internet violate the rights of recording artists? Or, is the recording industry attempting to unfairly restrict the opportunity for users to exchange and share information over the Internet? These and similar questions are examined in detail in this textbook.

Next, consider some ethical concerns affecting the cyberstalking incident involving Amy Boyer. Here, a wide range of ethical and social issues also arise, including concerns about privacy and security, free speech and censorship, and moral responsibility and legal liability. For example, was Boyer's privacy violated because of the way in which personal information about her could be so easily gathered by Liam Youens? Was Youens' ''right'' to set up a Web site about Amy Boyer without Boyer's knowledge, and without first getting her explicit consent, also a violation of Boyer's rights? And was Youens' alleged right to place on that Web site any kind of information about Boyer he wished to include, regardless of whether that information might be false or defamatory, a right that is protected by free speech? Should the two ISPs that allowed Youens to post such information to Web sites that reside in their Internet space be held legally liable? And should one of those ISPs be held liable, at least in

some contributory sense, for the murder of Amy Boyer, because of the death threat posted on one of the Web sites in its ''Internet space''? Do ordinary users who happen to come across a Web site that contains a posting of a death threat directed toward one or more individuals have a moral responsibility to inform those individuals whose lives are threatened?

The Verizon and the Amy Boyer cases each provide us with a context in which we can begin to think about a cluster of ethical issues affecting the use of computer and Internet technologies. A number of alternative examples could also have been used to illustrate many of the moral and legal concerns that arise because of the use of these and similar technologies. In fact, examples abound. Consider, for instance, the *MGM v. Grokster* case (2005) where the debate centered on whether Grokster, a peer-to-peer (P2P) network service, should be legally liable for copyright infringement for the proprietary movies and music exchanged on its system, and whether all P2P services should be forced to shut down because they *can* contribute to copyright infringement. Or consider the controversy surrounding the Bush Administration's efforts to subpoena the records of ordinary users' search queries made on the Google search engine during one week in the summer of 2005. Also, consider an incident that occurred in the spring of 2005 in which prospective graduate students ''hacked into'' their personal files that resided in a university's database in an effort to find out whether they had been admitted into the university's graduate program. These and other recent controversies involving cybertechnology are examined in detail in subsequent chapters of this textbook.

One has only to read a daily newspaper or view regular television news programs to be informed about controversial issues involving the Internet, including questions that pertain to property, privacy, security, anonymity, crime, and jurisdiction. Ethical aspects of each of these issues are examined in the chapters that comprise this textbook. In Chapter 1, we identify and examine some key foundational concepts in cyberethics.

▶ 1.1 DEFINING KEY TERMS: CYBERETHICS AND CYBERTECHNOLOGY

For our purposes, *cyberethics* can be defined as the study of moral, legal, and social issues involving cybertechnology. Cyberethics examines the impact of cybertechnology on our social, legal, and moral systems, and it evaluates the social policies and laws that have been framed in response to issues generated by its development and use. To grasp the significance of these reciprocal relationships, it is important to understand what is meant by the term *cybertechnology.*

1.1.1 What Is Cybertechnology?

Cybertechnology, as used throughout this textbook, refers to a wide range of computing and communications devices, from stand-alone computers to connected, or networked, computing and communications technologies. These technologies include, but need not be limited to, handheld devices such as Personal Digital Assistants (PDAs), personal computers (desktops and laptops), and mainframe computers. Networked devices can be connected directly to the Internet, or they can be connected to other devices through one or more privately owned computer networks. Privately owned networks, in turn, include Local Area Networks (LANs) and Wide Area Networks (WANs). A LAN is a privately

owned network of computers that span a limited geographical area, such as an office building or a small college campus. WANs, on the contrary, are privately owned networks of computers that are interconnected throughout a much broader geographic region.

How, exactly, are LANs and WANs different from the Internet? In one sense, the Internet can be understood as *the network of interconnected computer networks*. A synthesis of contemporary information and communications technologies, the Internet evolved from an earlier United States Defense Department initiative (in the 1960s) known as the ARPANET. Unlike WANs and LANs, which are privately owned computer networks, the Internet is generally considered to be a public network, in the sense that much of the information available on the Internet resides in ''public space'' and, thus, is available to anyone. The Internet, which should be differentiated from the World Wide Web, includes several applications. The Web, based on Hyper Text Transfer Protocol (HTTP), is one application; other applications include File Transfer Protocol (FTP), Telnet, and e-mail. Because many users access the Internet by way of the Web, and because the majority of users conduct their online activities almost exclusively on the Web portion of the Internet, it has become very easy to confuse the Web with the Internet.

The Internet and privately owned computer networks, such as WANs and LANs, are perhaps the most common and well known examples of *cybertechnology*. However, ''cybertechnology'' is used in this book to represent the entire range of computing systems, from stand-alone computers to privately owned networks to the Internet itself. And, ''cyberethics'' refers to the study of moral, legal, and social issues involving those technologies.

1.1.2 Why the Term ''Cyberethics''?

Many authors have used the term ''computer ethics'' to describe the field that examines moral issues pertaining to computing and information technology (see Moor, 2000; Johnson, 2001). Because of recent concerns about ethical issues involving the Internet in particular, some have also used the term ''Internet ethics'' (for example, Langford 2000). Ethical issues examined in this textbook, however, are not limited to the Internet or to computing machines; they also include privately owned computer networks and interconnected communications technologies—that is, technologies that we refer to collectively as ''cybertechnology.'' Hence we use ''cyberethics'' to capture the wide range of moral issues involving cybertechnology.

For our purposes, ''cyberethics'' is more accurate than either ''computer ethics'' or ''Internet ethics'' for two reasons: First, the term ''computer ethics'' can connote ethical issues associated with computing *machines*, and thus could be construed as pertaining to stand-alone or ''unconnected computers.'' Because computing technologies and communications technologies have converged in recent years, resulting in networked systems, a computer system may now be thought of more accurately as a new kind of *medium* than as a machine. Second, the term ''computer ethics'' might also suggest a field of study that is concerned exclusively with ethical issues involving computer professionals. Although these issues are very important, and are examined in detail in Chapter 4, we should note that the field of cyberethics is not limited to an analysis of moral issues that affect only professionals.

Given the wide range of moral issues examined in this book, the term ''cyberethics'' is also more comprehensive than ''Internet ethics.'' Although many of the issues considered

under the heading cyberethics often pertain to the Internet, some issues examined in this textbook do not involve the Internet per se; for example, issues associated with computerized monitoring in the workplace, with professional responsibility for designing reliable computer hardware and software systems, and with the implications of cybertechnologies for gender and race. We examine ethical issues that will cut across the spectrum of devices and networked communication systems comprising cybertechnology, from stand-alone computers to networked systems.

▶ 1.2 THE CYBERETHICS EVOLUTION: FOUR DEVELOPMENTAL PHASES

Cyberethics had its informal and humble beginnings in the late 1940s, when some analysts confidently predicted that not more than six computers would ever need to be built. Although still a relatively young field, cyberethics has now matured to a point where articles about its historical development have appeared in books and scholarly journals (see for example, Bynum 2004). For our purposes, the evolution of cyberethics can be summarized in four distinct *technological phases* (Tavani, 2001). Note that what we are calling a technological phase is not to be confused with something as precise as the expression ''computer generation,'' which is often used to describe specific stages in the evolution of computer hardware systems.

Phase 1 (1950s and 1960s), computing technology consisted mainly of huge mainframe computers that were unconnected and thus existed as stand-alone machines. One set of ethical and social questions raised during this phase had to do with the impact of computing machines as ''giant brains.'' Today, we might associate these kinds of questions with the field of artificial intelligence (AI). In Phase 1, the following kinds of questions arose: Can machines think? If so, should we develop thinking machines? If machines can be intelligent entities, what does this mean for our sense of self? What does it mean to be human?

Another set of ethical and social concerns that arose during Phase 1 could be catalogued under the heading of privacy and the fear of Big Brother. For example, some people in the United States feared that the federal government would set up a national database in which extensive amounts of personal information about its citizens could be stored as electronic records. A strong centralized government could then use that information to monitor and control the actions of ordinary citizens. Although networked computers had not yet come on to the scene, work on the ARPANET—the Internet's predecessor—began during this phase, in the 1960s.

In *Phase 2* (1970s and 1980s), computing machines and communications devices in the commercial sector began to converge. This convergence, in turn, introduced an era of computer/communications networks. Mainframe computers, minicomputers, microcomputers, and personal computers could now be linked together by way of one or more privately owned computer networks such as LANs and WANs (see Section 1.1.2), and information could readily be exchanged between and among databases accessible to networked computers. Ethical issues associated with this phase of computing involved personal privacy, intellectual property, and computer crime. Privacy concerns arose because electronic records containing personal and confidential information could easily be exchanged between two or more commercial databases, and concerns about intellectual property emerged because personal computers could be used to duplicate proprietary

software programs. Concerns involving computer crime appeared during this phase because individuals could now use computing devices, including remote computer terminals, to break into and disrupt the computer systems of large organizations.

During *Phase 3* (1990–present), the Internet era, availability of Internet access to the general public has increased significantly. This was facilitated, in no small part, by the development and phenomenal growth of the World Wide Web. The proliferation of Internet- and Web-based technologies has contributed to additional ethical concerns involving computing technology; for example, issues of free speech, anonymity, jurisdiction, and trust have been hotly disputed during this phase. Ethical and social concerns involving disputes over the public versus private character of personal information easily available on the Internet have also been introduced during Phase 3.

Presently we are on the threshold of *Phase 4,* a point at which we have begun to experience an unprecedented level of convergence of technologies. We have already witnessed technological convergence in Phase 2, where we saw the integration of computing and communications devices, resulting in privately owned networked systems. And in Phase 3, the Internet era, we saw the convergence of text, video, and sound technologies on the Web. The computer began to be viewed much more as a new kind of medium than as a conventional type of machine.

At Phase 3, both the interface used to interact with computer technology and the metaphor for understanding that technology were still much the same as in Phases 1 and 2. A computer was still essentially a box, a CPU, with one or more peripheral devices, such as video screen, keyboard, or mouse serving as an interface to that box. And computers were still viewed as devices essentially external to humans, as things or objects ''out there.''

As cybertechnology continues to evolve in Phase 4, it may no longer make sense to try to understand computers simply in terms of objects or devices that are necessarily external to us. Instead, computers will likely become more and more a part of who or what we are as human beings. For example, James Moor (2005) notes that computing devices will soon be a part of our clothing and even our bodies. Additionally, biochip implant technology, which has been enhanced by developments in AI research (described in Chapter 12), has led some to predict that in the not-too-distant future it may become difficult for us to separate certain aspects of our biology from our technology.

Also consider that computers are becoming ubiquitous and are beginning to ''pervade'' our work and recreational environments. Objects in these environments already, or very shortly will, exhibit what Philip Brey (2005) and others call ''ambient intelligence,'' which enables ''smart objects'' to be connected to one another via wireless technology. Some consider Radio Frequency Identification (RFID) technology (described in detail in Chapter 5) to be the first step in what some now refer to as *pervasive* or *ubiquitous* computing.

During Phase 4, many technologies that were previously distinct will most likely converge, and the pace at which technological convergence occurs will likely become accelerated. In recent years, the convergence of information technology and biotechnology has resulted in the emerging fields of bioinformatics and computational genomics. As a result, some now question whether current genetic/genomic research is still truly a biological science (that is, consisting of work in ''wet'' laboratories with chemicals). For example, we can ask whether it is more like computer science because much of the research is now carried out ''in silico,'' using digital representations of biological material. As convergence in the fields of biotechnology and information technology continues, it is

TABLE 1-1 Summary of Four Phases of Cyberethics

Phase	Time Period	Technological Features	Associated Issues
1	1950s–1960s	Stand-alone machines (large mainframe computers)	Artificial intelligence (AI), database privacy (''Big Brother'')
2	1970s–1980s	Minicomputers and PCs interconnected via privately owned networks	Issues from Phase 1 plus concerns involving intellectual property and software piracy, computer crime, privacy, and the exchange of records
3	1990s–present	Internet and World Wide Web	Issues from Phases 1 and 2 plus concerns about free speech, anonymity, legal jurisdiction, virtual communities, etc.
4	Present to near future	convergence of information and communication technologies with nanotechnology and biotechnology	Issues from Phases 1–3 plus concerns about artificial electronic agents (''bots'') with decision-making capabilities, and development in nanocomputing, bioinformatics, and computational genomics.

not clear whether computers of the future will still be silicon-based or whether they will possibly also be made of biological materials. Ethical concerns surrounding these and related questions, which are examined in Chapter 12, also arise as we proceed in Phase 4.

What other kinds of technological changes should we anticipate as research and development continues in Phase 4? Many predict that computers will become increasingly smaller in size, ultimately achieving the nanoscale. (We examine some of the ethical implications of nanotechnology and nanocomputing in Chapter 12.) Many also predict that nanotechnology, biotechnology, and information technology will continue to converge. However, in this chapter, we will not speculate any further about the future of cybertechnology or the future of cyberethics. The purpose of our brief description of the four phases of cyberethics mentioned here is to provide an historical context for understanding the origin and evolution of at least some of the ethical concerns affecting cybertechnology.

Table 1-1 summarizes key aspects of each phase in the development of cyberethics as a field of applied ethics.

▶ 1.3 ARE CYBERETHICS ISSUES UNIQUE ETHICAL ISSUES?

Few would dispute the claim that the use of cybertechnology has had a significant impact on our moral, legal, and social systems. Some also believe, however, that cybertechnology has introduced new and unique moral problems. Are any of these problems genuinely unique moral issues? There are two schools of thought regarding this question.

Consider once again the Amy Boyer cyberstalking case, illustrated in the chapter's opening section. Has this case introduced any new ethical issues, or has it merely exacerbated existing ones? One could argue that there is nothing really new or unique in the stalking case that led to Boyer's death, because in the final analysis ''crime is crime'' and ''murder is murder.'' According to this line of reasoning, whether a murderer happens to

use a computer to assist in carrying out a particular homicide is irrelevant. One might further argue that there is nothing special about cyberstalking incidents in general, regardless of whether or not they result in a victim's death. Proponents of this position could point to the fact that stalking activities are hardly new, because these kinds of activities have been carried out in the off-line world for quite some time. The use of computer and Internet technologies might be seen simply as the latest in a series of tools or techniques that are now available to aid stalkers in carrying out criminal activities.

Alternatively, some argue that forms of behavior made possible by cybertechnology have indeed raised either new or special ethical problems. Using the example of cyberstalking to support this view, one might point out the relative ease with which stalking activities can now be carried out: Simply by using a computing device with Internet access, one can stalk persons without having to leave the comfort of his or her home. A stalker can, as Liam Youens did, easily acquire personal information about his or her victim because such information is readily accessible to online search requests. Furthermore, a stalker can roam the Internet either anonymously or under the cloak of an alias, or pseudoname. The fact that a user can navigate the Web with relative anonymity makes it much more difficult for law enforcement agents to track down a stalker, either before or after that stalker has caused physical harm to the victim(s) (Grodzinsky and Tavani, 2004).

Also consider issues having to do with *scope* and *scale*: An Internet user can stalk multiple victims simultaneously via the use of multiple ''windows'' on his or her computer screen. The stalker can also stalk victims who happen to live in states and nations that are geographically distant from the stalker. Stalking activities can now occur on a scale or order of magnitude that could not have been realized in the pre-Internet era. More individuals can now engage in stalking behavior because cybertechnology has made it easy, and, as a result, significantly more people can now become the victims of stalkers.

But do these factors support the claim that cybertechnology has introduced any new and unique ethical issues? Walter Maner (2004) argues that computer use has generated a series of ethical issues that (a) did not exist before the advent of computing and (b) could not have existed if computer technology had not been invented. But is there any evidence to support Maner's claim? Next we consider two scenarios that, initially at least, might suggest that some new ethical issues have been generated by the use of cybertechnology.

▶ SCENARIO I: Designing a Controversial Computer System

One might argue that certain ethical issues involving design decisions facing computer professionals are unique because they never would have arisen had it not been for the invention of computer technology. For example, a software engineer might find herself in a situation where she must decide whether or not to participate in the design of a computer system that will likely be used to launch nuclear or chemical weapons. Is the ethical issue facing the engineer in this particular case new because it is peculiar to computer technology? In one sense, it is true that moral concerns having to do with whether or not one should participate in the design of a certain kind of computer system did not exist before the advent of computing technology. However, it is true only in a trivial sense. Clearly, since long before computing technologies were available, engineers have been faced with ethical choices involving whether or not to participate in the design and development of certain kinds of controversial technological systems. Prior to the computer era, they had to make decisions involving the design of aircraft intended to deliver conventional as well as nuclear bombs. So, is the fact that certain technological systems happen to include the use of computer software or computer hardware components morally relevant in this case?

Have any *new* or unique ethical issues, in a nontrivial sense of *unique*, been generated in this particular case? On the basis of our discussion of this scenario, there does not seem to be sufficient evidence to substantiate the claim that a new ethical issue has been introduced.

► **SCENARIO II:** Software Piracy

It might also be argued that ethical issues surrounding software piracy are new and thus unique to cybertechnology, because the art of pirating software programs would not have been possible if computer technology had not been invented in the first place. Once again, this claim would be true only in a trivial sense. The issue of piracy itself as a moral concern existed before the widespread use of computer technology. For example, people were able to pirate audiotapes simply by using two or more analog tape recorders to make unauthorized copies of proprietary material. The important point to note here is that moral issues surrounding the pirating of cassette tapes are, at bottom, the same issues underlying the pirating of computer software. They arise in each case because, fundamentally, the behavior associated with piracy raises moral concerns about property, fairness, rights, and so forth. So, as in Scenario I, there seems to be insufficient evidence to suggest that the ethical issues associated with software piracy are either new or unique in some nontrivial sense.

1.3.1 Distinguishing Between Unique Technological Features and Unique Ethical Issues

On the basis of our analysis of the two scenarios in the preceding section, we might conclude that there is nothing new or special about the kinds of moral issues associated with cybertechnology. In fact, some philosophers have argued that we have the same old ethical issues reappearing in a new guise. But is such a view accurate?

If we focus primarily on the moral issues themselves *as moral issues*, it would seem that perhaps there is nothing new. Cyber-related concerns involving privacy, property, free speech, etc., can be understood as specific expressions of core (traditional) moral notions, such as autonomy, fairness, justice, responsibility, and respect for persons. However, if instead we focus more closely on cybertechnology itself, we see that there are some interesting and possibly unique features that distinguish this technology from earlier technologies. Maner has argued that computing technology is ''uniquely fast,'' ''uniquely complex,'' and ''uniquely coded.'' But even if cybertechnology has these unique features, does it necessarily follow that any of the moral questions associated with them must also be unique? One would commit a logical fallacy if he or she concluded that cyberethics issues must be unique simply because certain features or aspects of cybertechnology are unique (Tavani, 2002). The fallacy can be expressed in the following way:

Cybertechnology has some unique technological features;

Cybertechnology has generated ethical issues;

Therefore, ethical issues generated by cybertechnology must be unique ethical issues.

As we will see in Chapter 3, this reasoning is fallacious because it assumes that characteristics that apply to a certain technology must also apply to ethical issues associated with that technology.

1.3.2 An Alternative Strategy for Analyzing the Question About Uniqueness

Although it may be difficult to prove conclusively whether or not cybertechnology has generated any new or unique ethical issues, we must not rule out the possibility that many of the controversies associated with this technology might warrant special consideration from an ethical perspective. But what exactly is so different about issues involving cybertechnology that makes them deserving of special moral consideration? James Moor (2000) points out that computer technology, unlike most previous technologies, is ''logically malleable''; it can be shaped and molded to perform a variety of functions. Because noncomputer technologies are typically designed to perform some particular function or task, they lack the universal or general-purpose characteristics that computing technologies possess. For example, microwave ovens and DVD players are technological devices that have been designed to perform specific tasks. Microwave ovens cannot be used to view DVDs, and DVD players cannot be used to defrost, cook, or reheat food. However, a computer, depending on the software used, can perform a range of diverse tasks: It can be instructed to behave as a video game, a word processor, a spreadsheet, a medium to send and receive e-mail messages, or an interface to Web sites. Hence, cybertechnology is extremely malleable.

Moor points out that because of its logical malleability, cybertechnology can generate ''new possibilities for human action'' that appear to be limitless. Some of these possibilities for action generate what Moor calls ''policy vacuums,'' because we have no explicit policies or laws to guide new choices made possible by computer technology. These vacuums, in turn, need to be filled with either new or revised policies. But what exactly does Moor mean by ''policy''? Moor (2004) defines policies as ''rules of conduct, ranging from formal laws to informal, implicit guidelines for actions.'' Viewing computer-ethics issues in terms of policies is useful, Moor believes, because policies have the right level of generality to consider when we evaluate the morality of conduct. As noted, policies can range from formal laws to informal guidelines. Moor also notes that policies can have justified exemptions because they are not absolute; yet policies usually imply a certain ''level of obligation'' within their contexts.

What action is required when one or more policy vacuums are discovered? A solution to this problem might seem quite simple and straightforward. For example, we might assume that all we need to do is identify the vacuums that have been generated and then fill them with policies and laws. However, this will not always work, because sometimes the new possibilities for human action generated by cybertechnology also introduce ''conceptual vacuums,'' or what Moor calls ''conceptual muddles.'' In these cases, we must first eliminate the muddles by clearing up certain conceptual confusions before we can frame coherent policies and laws.

▶ CASE ILLUSTRATION OF A POLICY VACUUM: Duplicating Computer Software

One significant policy vacuum, which also involved a conceptual muddle, emerged with the advent of personal desktop computers (henceforth referred to generically as PCs). The particular vacuum arose because of the controversy surrounding the copying of software. When PCs became commercially available, many users discovered that they could easily duplicate software programs. They found that they could use their PCs to make copies of proprietary computer programs such as word processing programs, spreadsheets, and video games. Some users assumed that in making copies of these programs they were doing nothing wrong. At that time, there were no explicit laws to regulate the

subsequent use and distribution of software programs once they had been legally purchased by an individual or by an institution. Although it might be difficult to imagine today, at one time software was not clearly protected by either copyright law or the patent process.

Of course, there were clear laws and policies regarding the theft of physical property. Such laws and policies protected against the theft of personal computers as well as against the ''theft'' of a physical disk drive residing in a PC on which the proprietary software programs could easily be duplicated. However, this was not the case with laws and policies regarding the theft, or unauthorized copying of software programs that resided on computers. Although there were intellectual property laws in place, it had not been determined that software was or should be protected by intellectual property (IP) law: It was unclear whether software should be understood as an idea (which is not protected by IP law), as a form of writing protected by copyright law, or as a set of machine instructions protected by patents. Consequently, many entrepreneurs who designed and manufactured software programs argued for explicit legal protection for their products. A policy vacuum arose with respect to duplicating software: Could a user make a backup copy of a program for oneself? Could one share it with a friend? Could one give the original program to a friend? A clear policy was needed to fill this vacuum.

Before we can fill the vacuum regarding software duplication with a coherent policy or law, we first have to resolve a certain conceptual muddle by answering the following question: What exactly is computer software? Until we can clarify the concept of software itself, we cannot frame a coherent policy as to whether or not we should allow the free duplication of software. Currently there is still much confusion, as well as considerable controversy, as to how laws concerning the exchange (and, in effect, duplication) of proprietary software over the Internet should be framed.

In Moor's scheme, how one resolves the conceptual muddle or decides the conceptual issue can have a significant effect on which kinds of policies are acceptable. Getting clear about the conceptual issues is an important first step, but it is not a sufficient condition for being able to formulate a policy. Finally, the justification of a policy requires much factual knowledge, as well as an understanding of normative and ethical principles.

Consider the controversy involving the original Napster Web site and the Recording Industry Association of America. Proponents on both sides in the Napster dispute experienced difficulties in making convincing arguments for their respective positions due, in no small part, to confusion regarding the nature and the status of information being exchanged between Internet users and the technology that facilitated this exchange. Although cybertechnology has made it possible to exchange MP3 files, there is still a debate, and arguably a great deal of confusion as well, about whether doing so should necessarily be illegal. Until some of the conceptual confusions or muddles underlying arguments used in the Napster case in particular, and about the nature of P2P file-sharing systems in general, are resolved, it is difficult to imagine how a satisfactory policy regarding the exchange of MP3 files in P2P transactions can be framed.

How, exactly, does Moor's insight that cyberethics issues need to be analyzed in terms of potential policy vacuums and conceptual muddles contribute to our earlier question as to whether there is anything unique or special about cyberethics? First, we should note that Moor takes no explicit stance on the question as to whether any cyberethics issues are unique. However, he does argue that cyberethics issues deserve special consideration because of the nature of cybertechnology itself, which is significantly different from

alternative technologies in terms of the vast number of policy vacuums it generates (Moor, 2001). So even though the ethical issues—that is, issues involving privacy, intellectual property, and so forth—might not be new or unique, they nonetheless can put significant pressure on our conceptual frameworks and normative reasoning to a degree not found in other areas of applied ethics. Thus, it would seem to follow, on Moor's line of reasoning, that an independent field of applied ethics that focuses on ethical aspects of cybertechnology is indeed justified.

▶ 1.4 CYBERETHICS AS A BRANCH OF APPLIED ETHICS: THREE DISTINCT PERSPECTIVES

Cyberethics, as a field of study, can be understood as a branch of *applied ethics*. Applied ethics, as opposed to theoretical ethics, examines practical ethical issues. It does so by analyzing those issues from the vantage point of one or more ethical theories. Whereas ethical theory is concerned with establishing logically coherent and consistent criteria in the form of standards and rules for evaluating moral problems, the principal aim of applied ethics is to analyze specific moral problems themselves through the application of ethical theory. As such, those working in fields of applied ethics are not inclined to debate some of the finer points of individual ethical theories. Instead, their interest in ethical theory is primarily with how one or more theories can be successfully applied to the analysis of specific moral problems that they happen to be investigating.

For an example of a practical-ethics issue involving cybertechnology, consider again the original Napster controversy (see Section 1.3.2). Recall that at the heart of this dispute is the question of whether the exchange of proprietary software, in a digital format known as MP3, over the Internet should be permitted. Those advocating the free exchange of MP3 files could appeal to one or more ethical theories to support their position. For example, they might appeal to utilitarianism, an ethical theory that is based on the principle that our policies and laws should be such that they produce the greatest good (happiness) for the greatest number of people. A utilitarian might argue that MP3 files should be distributed freely over the Internet because the consequences of allowing such a practice would make the majority of users happy and would thus contribute to the greatest good for the greatest number of persons affected.

Others might argue that allowing this proprietary material to be exchanged freely over the Internet would violate the rights of those who created, and who legally own, the material. Proponents of this view could appeal to a nonutilitarian principle or theory that is grounded in the notion of respecting the rights of individuals. According to this view, the concern is with protecting the rights of individuals who legally own the proprietary material in question, irrespective of the happiness that might or might not result for the majority of Internet users.

Notice that in the case involving the dispute over the exchange of MP3 files on the Internet, the application of two different ethical theories yields two very different answers to the question of which policy or course of action ought to be adopted. Sometimes, however, the application of different ethical theories to a particular problem will yield similar solutions. We will examine in detail some standard ethical theories, including utilitarianism, in Chapter 2. Our main concern in this textbook is with applied, or practical, ethics issues,

and not with ethical theory per se. Wherever appropriate, however, ethical theory will be used to inform our analysis of moral issues involving cybertechnology.

Understanding cyberethics as a field of applied ethics that examines moral issues pertaining to cybertechnology is an important first step. But much more needs to be said about the perspectives that interdisciplinary researchers bring to their analysis of the issues that make up this relatively new field. Most scholars and professionals conducting research in this field of applied ethics have proceeded from one of three different perspectives—professional ethics, philosophical ethics, or descriptive ethics. Gaining a clearer understanding of what is meant by each of these perspectives is useful at this point.

1.4.1 Perspective #1: Cyberethics as a Field of Professional Ethics

According to those who view cyberethics primarily as a branch of *professional ethics*, the field can best be understood as identifying and analyzing issues of ethical responsibility for computer professionals. Among the cyberethics issues considered from this perspective are those having to do with the computer professional's role in designing, developing, and maintaining computer hardware and software systems. Suppose a programmer discovers that a software product she has been working on is about to be released for sale to the public even though that product is unreliable because it contains ''buggy'' software. Should she blow the whistle?

Those who see cyberethics essentially as a branch of professional ethics would likely draw on analogies from other professional fields, such as medicine and law. They would point out that in medical ethics and legal ethics, the principle focus of analysis is on issues of moral responsibility that affect individuals as *members* of those professions. By analogy, they would go on to argue that the same rationale should apply to the field of cyberethics: The primary, and possibly even exclusive, focus of cyberethics should be on issues of moral responsibility that affect computer professionals.

Don Gotterbarn (1995), who has argued for the view that cyberethics is best understood as a field of professional ethics, has suggested that the principal focus of computer ethics should be on issues of professional responsibility and not on the broader moral and social implications of that technology. The analogies used in his argument are instructive. Gotterbarn notes, for example, that in the past certain technologies have profoundly altered our lives, especially in the ways that many of us conduct our day-to-day affairs. Consider three such technologies: the printing press, the automobile, and the airplane. Despite the significant and perhaps revolutionary effects of each of these technologies, we do not have ''printing press ethics,'' ''automobile ethics,'' or ''airplane ethics.'' So why, Gotterbarn asks, should we have a field of computer ethics apart from the study of those ethical issues that affect the professionals responsible for the design, development, and delivery of computer systems? In other words, Gotterbarn suggests that it is not the business of computer ethics to examine ethical issues other than those that affect computer professionals.

Professional Ethics and the Computer Science Practitioner

Gotterbarn's view about what the proper focus of computer ethics research and inquiry should be is shared by other practitioners in the discipline of computer science (see, for

example, Baase, 2003). However, some of those practitioners, as well as many philosophers and social scientists, believe that Gotterbarn's conception of computer ethics simply as a field of professional ethics is too limited or too narrow. In fact, some who identify themselves as computer professionals or as information professionals, and who are otherwise sympathetic to Gotterbarn's overall attention to professional ethics issues, believe that that a broader model is needed. Elizabeth Buchanan (2004), who also recognizes the important role of the analysis of ethical issues involving the ''information professions,'' suggests that the study of cyberethics issues must include an examination of many nonprofessional-ethics issues as well. In describing the field of information ethics as one that affects information professionals, Buchanan also suggests that the issues involving information ethics have a significant impact on ordinary computer users as well. In fact, we should note that these issues also affect people who have never even used a computer.

Of course, Buchanan's category of ''informational professional'' is considerably broader in scope than Gotterbarn's notion of computer professional. But the central point of her argument still holds, especially in the era of the Internet and the World Wide Web. In the computing era preceding the Web, Gotterbarn's conception of the field as one limited to ethical issues concerning computer professionals might have seemed more appropriate than it does today. Now, computers are virtually everywhere, and the ethical issues generated by cybertechnology affect virtually everyone, professional and nonprofessional, alike. However, in spite of – and perhaps even because of – this factor, Gotterbarn's conception of the field may turn out to be correct. We next consider how this possible.

As cybertechnology increasingly pervades our surroundings and as it continues to mediate our everyday behavior and activities, computers are beginning to ''disappear'' by blending into our environments and are thus becoming less conspicuous as some thing or object. (Recall our description of Phase IV of cybertechnology in Section 1.2.) Deborah Johnson (2000) believes that in the future, many computer-related ethical issues, such as those affecting privacy and property (which are currently associated with the field of computer ethics), may become part of what she calls ''ordinary ethics.'' In fact, Johnson has suggested that computer ethics, as a separate field of applied ethics, may eventually go away because its issues will be folded into ordinary ethics. However, even if Johnson's prediction turns out to be correct, computer ethics as a field that examines ethical issues affecting responsibility for computer professionals will, in all likelihood, still be needed. In this sense, then, Gotterbarn's original model of computer ethics might prove to be the correct one in the long term.

Applying the Professional Ethics Model to Cyberethics Issues

It is fairly easy to see how the professional-ethics model can be used to analyze issues involving professional responsibility that directly impact computer professionals. For example, issues concerned with the development and implementation of reliable software would fit closely with the professional model. But can that model be extended to include cases that may only affect computer professionals indirectly?

We can ask how some of the issues in the Verizon and the Amy Boyer cyberstalking cases, both described earlier in this chapter, might be analyzed from the perspective of professional ethics. First consider the Verizon case, which initially might seem outside the purview of computer ethics vis-à-vis professional ethics. Yet some interesting and

controversial questions arise that have implications for computer professionals. For example, should programmers design systems that allow commercial organizations such as the recording industry to engage in the surveillance of online activities of ordinary users? Should programmers be prohibited from designing P2P applications because they can be abused by some individuals in illicit file-sharing activities? Questions such as these clearly have an impact for computer professionals.

Next consider the Boyer case. From the vantage point of professional ethics, one might argue that cyberstalking in general and the murder of Amy Boyer in particular are not the kinds of concerns that are the proper business of computer ethics. We saw that someone like Gotterbarn might ask why a crime that happened to involve the use of a computer should necessarily be construed as an issue for computer ethics. For example, he notes that a murder that happened to be committed with a surgeon's scalpel would not be considered an issue for medical ethics. Although murders involving the use of a computer, like all murders, are serious moral and legal problems, Gotterbarn seems to imply that they are not examples of genuine computer-ethics issues.

However, Gotterbarn and the advocates for his position are acutely aware that software developed by engineers can have implications that extend far beyond the computing profession itself. So, for example, engineers who develop code that can be used in applications that violate individual privacy may bear some of the responsibility for harms caused by that code. And ISPs that use those software applications could also share some responsibility for privacy violations. Thus, someone approaching the Amy Boyer case from the perspective of professional ethics might ask the following kinds of questions: Was Boyer's right to privacy violated? If so, should the ISPs involved be held morally responsible or legally liable? And should the computer professionals who are employed by those ISPs, or who developed the software code that enabled Boyer's privacy to be violated, also be held responsible?

Many of the ethical issues discussed in this book have implications for computer professionals, either directly or indirectly. Issues that have a direct impact on computer professionals in general, and software engineers in particular, are examined in Chapter 4, which is dedicated to professional ethics. Computer science students and computer professionals will probably also want to assess some of the indirect implications that issues examined in Chapters 5 through 12 have for the computing profession.

1.4.2 Perspective #2: Cyberethics as a Field of Philosophical Ethics

What exactly is *philosophical ethics* and how is it different from professional ethics? Because philosophical methods and tools are also used to analyze issues involving professional ethics, any attempt to distinguish between the two might seem arbitrary, perhaps even odd. For our purposes, however, a useful distinction can be drawn between the two fields because of the approach each takes in addressing ethical issues. Whereas professional-ethics issues typically involve concerns of responsibility and obligation affecting individuals as members of a certain profession, philosophical ethics issues include broader concerns—social policies as well as individual behavior—that affect virtually everyone in society. Cybertechnology-related moral issues involving privacy, security, property, and free speech can affect everyone, including individuals who have never even used a computer.

To appreciate the perspective on cyberethics as a field of philosophical ethics, consider James Moor's classic definition of computer ethics. According to Moor (2000), computer ethics is

> *the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology.* [Italics added.]

Two points in Moor's definition are worth examining more closely. First, computer ethics (i.e., what we call ''cyberethics'') is concerned with the social impact of computers and cybertechnology in a broad sense and not merely with the impact of that technology for computer professionals. Second, this definition challenges us to reflect on the social impact of cybertechnology in a way that requires a justification for our social policies.

Why is cyberethics, as a field of philosophical ethics dedicated to the study of ethical issues involving cybertechnology, warranted when there are not similar fields of applied ethics for other technologies? Recall our earlier discussion of Gotterbarn's observation that we do not have fields of applied ethics called ''automobile ethics'' or ''airplane ethics,'' even though automobile and airplane technologies have significantly affected our day-to-day lives. Moor would disagree with Gotterbarn on this point, even though Moor does not deny that the professional-responsibility issues identified by Gotterbarn must also be taken into account. But how would Moor respond to Gotterbarn's central argument about the social impact of previous technologies and their connection (or lack of one) to ethics?

Moor notes that the introduction of automobile and airplane technologies did not affect our social policies and norms in the same kinds of fundamental ways that computer technology has. Of course, we have had to modify and significantly revise certain laws and policies to accommodate the implementation of new kinds of transportation technologies. In the case of automobile technology, we had to extend, and in some cases modify, certain policies and laws previously used to regulate the flow of horse-drawn modes of transportation. And clearly, automobile and airplane technologies have revolutionized transportation, resulting in our ability to travel faster and farther than was possible in previous eras.

What has made the impact of computer technology significantly different from that of other modern technologies? We have already seen that for Moor, three factors contribute to this impact: logical malleability, policy vacuums, and conceptual muddles. Because cybertechnology is logically malleable, its uses often generate policy vacuums and conceptual muddles. In Section 1.3.2, we saw how certain kinds of conceptual muddles contributed to some of the confusion surrounding software piracy issues in general, and the Napster controversy in particular. What implications do these factors have for the standard methodology used by philosophers in the analysis of applied ethics issues?

Methodology and Philosophical Ethics

According to Philip Brey (2004), the standard methodology used by philosophers to conduct research in applied ethics has three distinct stages in that an ethicist must

1. identify a particular controversial practice as a moral problem,
2. describe and analyze the problem by clarifying concepts and examining the factual data associated with that problem,
3. apply moral theories and principles in the deliberative process in order to reach a position about the particular moral issue.

We have already noted (in Section 1.3) how the first two stages in this methodology can be applied to an analysis of ethical issues associated with cyberpiracy. We saw that first, a practice involving the use of cybertechnology to ''pirate'' or make unauthorized copies of proprietary information was *identified* as morally controversial. At the second stage, the problem was *analyzed* in descriptive and contextual terms to clarify the practice and to situate it in a particular context. In the case of cyberpiracy, we saw that the concept of piracy could be analyzed in terms of moral issues involving theft and intellectual property theory. When we describe and analyze problems at this stage, we will want to be aware of and address any policy vacuums and conceptual muddles that are relevant.

At the third and final stage, the problem must be *deliberated* over in terms of moral principles (or theories) and logical arguments. Brey describes this stage in the method as the ''deliberative process.'' Here, various arguments are used to justify the application of particular moral principles to the issue under consideration. For example, issues involving cyberpiracy can be deliberated upon in terms of one or more standard ethical theories, such as utilitarianism (defined in Chapter 2).

Applying the Method of Philosophical Ethics to the Verizon and the Amy Boyer Cases
To see how the philosophical-ethics perspective of cyberethics can help us to analyze cyber-related moral issues other than digital piracy, we can revisit the *Verizon v. RIAA* case and the cyberstalking case involving Amy Boyer. Our first task is to identify one or more moral issues associated with each case. We have already seen that both raise several ethical issues. For example, among the ethical issues identified in the Verizon case were concerns affecting privacy, anonymity, surveillance, and intellectual property (Grodzinsky and Tavani, 2005). We can now ask whether any policy vacuums and conceptual muddles were generated in that case. We noted earlier that the original Napster case introduced controversies with respect to sharing proprietary MP3 files online. The Verizon case, however, introduces some issues that go beyond that concern. For example, what is an ISP user's expectation of privacy and anonymity while engaged in online activities? Is it permissible for commercial organizations such as the recording industry to monitor an individual's online activities, even when it suspects a user of exchanging proprietary files containing music or movies? Does the recording industry's behavior in this case violate any basic civil liberties guaranteed in the U.S. Constitution? The courts, thus far, have vacillated in their interpretation of these questions. So, arguably, a policy vacuum has emerged with respect to whether commercial organizations such as the RIAA should to be allowed to engage in surveillance activities regarding the users of P2P systems and whether they should be able to require that ISPs disclose the identities of their subscribers.

Next consider the Boyer case. Recall that one of the ethical concerns we identified in that case of cyberstalking had to do with personal privacy; among the complaints in the wrongful death suit filed by Amy Boyer's stepfather was that his stepdaughter's privacy had been violated. We next ask whether the specific privacy concerns involving the Boyer case have generated any policy vacuums or conceptual muddles. Note that the kind of personal information about Boyer that her stalker was able to retrieve from the Internet would probably be considered ''public information,'' given that much of it was also accessible in public records. Of course, it is now much easier to access public records because of their online availability, in many instances, than it was in the precomputer era; so we might now ask whether our existing privacy laws and policies regarding the access and flow of personal

information are still adequate. In other words, does a policy vacuum exist here? The fact that personal information residing in public databases can now be accessed with relative ease through the use of Internet search facilities would seem to pose a challenge for our existing privacy policies. It would also seem that a policy vacuum has emerged here.

Next, we ask whether any conceptual vacuums or muddles have also been introduced. Consider criteria that we have traditionally used to distinguish between personal information that is essentially public and personal information that is considered private in nature. Is there also conceptual muddle here? That is, does the concept of personal information itself need to be reexamined in an age of cybertechnology? (We will address this particular question in Chapter 5, where we examine a set of privacy concerns that some now refer to as the ''problem of privacy in public.'' We will see that our traditional conception of privacy, which has informed our current policies, may indeed need to be rethought in light of vacuums introduced by cybertechnology.) Once the policy vacuums and conceptual muddles have been resolved, we can then move on to the third and final stage, where we deliberate on how best to resolve the privacy issue involving the Boyer case. In our discussion of ethical theory in Chapter 2, we will see how this is done.

1.4.3 Perspective #3: Cyberethics as a Field of Descriptive Ethics

We have examined two perspectives on cyberethics that can both be understood as *normative* inquiries into applied ethics issues. Normative inquiries or studies, which focus on evaluating and prescribing moral systems, can be contrasted with *descriptive* inquiries or studies. Descriptive ethics describes aspects of particular moral systems and reports how members of various groups and cultures view particular moral issues. Whereas descriptive investigations provide us with information about what *is* the case, normative inquiries evaluate situations from the vantage point of questions having to do with what *ought to be* the case.

Those who approach cyberethics from the perspective of descriptive ethics often describe sociological aspects of a particular moral issue, such as the social impact of a certain technology on a certain community. For example, one way of analyzing moral issues surrounding the ''digital divide'' (examined in Chapter 10) is first to describe the problem in terms of its impact on various sociodemographic groups involving social class, race, and gender. We can then investigate whether, in fact, fewer poor people, nonwhites, and women have access to cybertechnology than wealthy and middle-class persons, whites, and men. In this case, the investigation is one that is basically descriptive in character. If we were then to inquire whether the lack of access to technology for some groups relative to others was unfair, we would be engaging in a normative inquiry. For example, a normative investigation of this issue would question whether certain groups *should* have more access to cybertechnology than they currently have. The following scenario illustrates an approach to a particular cyberethics issue via the perspective of descriptive ethics.

▶ **SCENARIO III:** Describing the Impact of a Technology on a Community's Workforce

Imagine that a major employer in a certain community decides to implement a new kind of computer/information technology in the workplace. Further imagine that the implementation of this new technology has significant social implications for the community. If we analyze the impact that this

new technology has with respect to the number of jobs that are gained or lost in that community, our investigation is essentially descriptive in nature. For example, imagine that since the introduction of Technology X, 8000 workers in Community Y have lost their jobs. In reporting this phenomenon, we are simply describing an impact that the introduction of Technology X has for Community Y.

This inquiry and analysis of the issue in Community Y involves nothing more than simply describing what *is* the case. If, however, we argue that those workers *ought not* to have been displaced, then we make a claim that is normative. For example, one might argue that the workers should not have been displaced because of certain contractual obligations between the employer and its employees. Or we might argue that certain additional factors should have been taken into consideration when determining which workers would lose their jobs. Suppose that in the process of eliminating jobs, older workers and minority employees were disproportionately affected. Would that have affected the way we view the situation?

Our first account of the social impact of the new technology on workers in Community Y simply reported to us some information about the number of jobs lost to workers in that community. In the latter account, however, we did much more than merely describing what the impact was. There, we were also evaluating certain aspects of that impact for Community Y in terms of what we believed *ought* to have been done. In doing so, we shifted from an analysis of a social impact in terms of claims that were merely descriptive to an analysis in which the claims were essentially normative.

Descriptive Versus Normative Claims

To further illustrate the differences between claims that are normative and those that are descriptive, consider the following three assertions involving Bill Gates:

1. Bill Gates served as the Chief Executive Officer of Microsoft Corporation for many years.
2. Bill Gates should expand Microsoft's product offerings.
3. Bill Gates should engage in business practices that are fair to competitors.

As you might already have inferred, one of the claims is descriptive and two are normative. A person asserting (1) has made a descriptive claim about Gates. Someone asserting either (2) or (3), however, makes a normative claim. Assertions (2) and (3) are normative because they contain evaluative terms such as ''should'' and ''ought.'' As such, these two assertions do more than merely report something about Gates in purely descriptive terms.

It is important to point out that not every normative claim is also a moral claim. For example, the normative assertions expressed in (2) and (3) are different in at least one very significant respect. Even though both assertions are normative, only (3) is also a moral assertion. We will consider the normative/descriptive distinction, as well as the distinction between moral and nonmoral normative claims, in greater detail in Chapter 2.

Figure 1-1 illustrates some differences between normative and descriptive assertions.

Some Benefits of Using the Descriptive Approach to Analyze Cyberethics Issues

How, exactly, is the examination of cyberethics issues from the perspective of descriptive ethics useful? For one thing, many sociologists and social scientists working in the field of

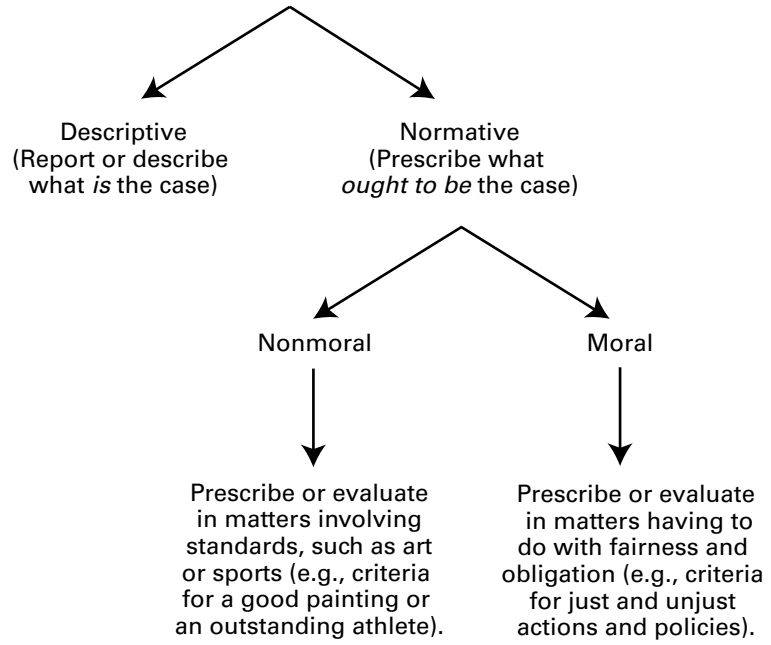

Figure 1-1 Descriptive Versus Normative Claims

cyberethics believe that focusing initially on descriptive aspects of these issues can help us to better understand certain normative features and implications. For example, Chuck Huff and Thomas Finholt (1994) have argued that when we understand the social effects of technology in its descriptive sense, the normative ethical questions become clearer. An analysis of the social impact of cybertechnology in descriptive terms is useful for at least two reasons: First, approaching questions from the descriptive perspective can prepare us better for our subsequent analysis of practical ethical issues affecting our system of policies and laws. Second, the descriptive approach can help computer professionals in their attempts to design computer systems that might avoid social and ethical problems associated with earlier computer systems. So, using Huff and Finholt's model, we can see how the descriptive-ethics perspective can work in conjunction with the goals and objectives of both practical ethics and professional ethics.

We have already noted that virtually all of our social institutions, from work to education to government to finance, have been affected by cybertechnology. This technology has also had significant impacts on different sociodemographic sectors and segments of our population. The descriptive information that we gather about these groups can provide important information that, in turn, can inform legislators and policy makers who are drafting and revising laws in response to the effects of cybertechnology.

From the perspective of descriptive ethics, we are also better able to examine the impact that cybertechnology has for our notions of community and democracy. We can ask, for instance, whether certain developments in virtual-reality technology have affected the way that we conceive traditional notions such as ''community'' and ''neighbor.'' Is a community essentially a group of individuals with similar interests and perhaps a similar ideology,

irrespective of geographical limitations? Is national identity something that is, or may soon become, anachronistic? Although these kinds of questions and issues in and of themselves are more correctly conceived as descriptive rather than normative concerns, they can have significant normative implications for our moral and legal systems as well. Much more will be said about the relationship between descriptive and normative approaches to analyzing ethical issues in Chapter 10, where we will examine the impact of cybertechnology on sociodemographic groups and on many of our social and political institutions.

Applying the Descriptive Ethics Approach to the Verizon and the Amy Boyer Cases

Consider how someone approaching cyberethics issues from the perspective of descriptive ethics might analyze the *Verizon v. RIAA* case and the cyberstalking case involving Amy Boyer. In analyzing the Verizon case, sociologists might focus their attention on concerns involving ''social control'' on the part of nongovernmental organizations, such as the recording industry. For example, they might analyze this case from the point of view of user participation in P2P networks to see whether there has been a significant change in the behavior of those who currently use these forums, and whether certain groups are affected more than others, as a result of the recording industry's activities. They might also conduct surveys to see whether, as a result of the RIAA's threats and lawsuits, individuals have a greater fear about sharing music in P2P systems.

Next consider the Boyer case. For one thing, someone analyzing this incident from the point of view of descriptive ethics might inquire into whether there has been an increase in the number of stalking and stalking-related criminal activities. And if the answer to this question is ''yes,'' next she might question whether such an increase is linked to the widespread availability of cybertechnology. Also, she might consider whether certain groups in the population are now more at risk than others with respect to being stalked in cyberspace. She could inquire whether there are any statistical patterns to suggest that celebrities and certain high-profile individuals, such as politicians and corporate leaders, are more likely to be stalked via cybertechnology than are ordinary individuals. She could ask if women are generally more vulnerable to the kinds of threats posed by cyberstalking than men. And, if they are, then are younger, single women more likely to be stalked in cyberspace than women in other subgroups?

Also, a researcher approaching the Boyer case from the descriptive-ethics perspective might set out to determine whether a profile for a typical cyberstalker can be established. The researcher might pursue answers to the following kinds of questions: Is a typical cyberstalker someone who is young, white, and male? Is it likely that individuals who never would have thought of physically stalking a victim in geographical space might now be inclined to engage in cyberstalking, perhaps because of the relative ease of doing so with cybertechnology? Or is it the case that some of those same individuals might now be tempted to do so because they believe that they will not likely get caught? Also, has the fact that a potential cyberstalker realizes that he or she can stalk a victim on the Internet under the cloak of relative anonymity contributed to the increase in stalking-related activities? These are a few of the kinds of questions that could be examined from the descriptive perspective of cyberethics.

Table 1-2 summarizes some key characteristics that differentiate the three main perspectives for approaching cyberethics issues.

In Chapters 4–12, we examine specific cyberethics questions from the vantage points of three perspectives: Issues considered from the perspective of professional ethics are

TABLE 1-2 Summary of Cyberethics Perspectives

Type of Perspective	Associated Disciplines	Issues Examined
Professional	Computer Science Engineering Library/Information Science	Professional responsibility System reliability/safety Codes of conduct
Philosophical	Philosophy Law	Privacy and anonymity Intellectual property Free speech
Descriptive	Sociology Behavioral Sciences	Impact of cybertechnology on governmental/financial/educational institutions and sociodemographic groups

examined in Chapter 4. Cyberethics issues considered from the perspective of philosophical ethics, such as those involving privacy, security, and intellectual property and free speech, are examined in Chapters 5 through 9. And several of the issues considered in Chapters 10 and 11 are examined from the perspective of descriptive ethics.

▶ 1.5 A COMPREHENSIVE CYBERETHICS METHODOLOGY

The three different perspectives of cyberethics described in the preceding section might suggest that three different kinds of methodologies are needed to analyze the range of issues examined in this textbook. The goal of this section, however, is to show that a single, comprehensive method can be constructed and that this method will be adequate in guiding us in our analysis of cyberethics issues.

Recall the standard model used in applied ethics, which we briefly examined in Section 1.4.2. There we saw that the standard model includes three stages in which a researcher must (1) identify an ethical problem, (2) describe and analyze the problem in conceptual and factual terms, and (3) apply ethical theories and principles in the deliberative process. We also saw that Moor (2000) argued that the conventional model was not adequate for an analysis of at least some cyberethics issues. Moor believed that additional steps, which addressed concerns affecting ''policy vacuums'' and ''conceptual muddles,'' are sometimes needed before we can move from the second to the third stage of the methodological scheme. We must now consider whether the standard model, with Moor's additional steps included, is complete. Brey (2004) suggests that it is not.

Brey believes that while the (revised) standard model might work well in many fields of applied ethics, such as medical ethics, business ethics, and bioethics, it does not always fare well in cyberethics. Brey argues that the standard method, when used to identify ethical aspects of cybertechnology, tends to focus almost exclusively on the *uses* of that technology. As such, the standard method fails to pay sufficient attention to certain features that may be embedded in the technology itself, such as design features that may also have moral implications.

We might be inclined to assume that technology itself is neutral and that only the uses to which a particular technology is put are morally controversial. However, Brey and others

believe that it is a mistake to conceive of technology, independent of its uses, as something that is value free, or unbiased. Instead, they argue, moral values are often embedded or implicit in features built into technologies at the design stage. For example, some feminist critics have pointed out that in the past, the ergonomic systems designed for drivers of automobiles were biased toward men and gave virtually no consideration to women. That is, considerations having to do with the average height and typical body dimensions of men were implicitly built into the design specification. These critics also note that decisions about how the ergonomic systems would be designed were all made by men, which likely accounts for the bias embedded in that particular technological system.

1.5.1 Is Cybertechnology Neutral?

As noted in the preceding section, Brey believes that cybertechnology has certain built-in values and biases that are not always obvious or easy to detect. He worries that these biases can easily go unnoticed by computer ethics researchers. An example of how difficult it can be to detect relevant biases and values can be found in a case outside cybertechnology, namely, gun technology. You have probably heard the expression, ''Guns don't kill people; people kill people.'' An assumption underlying this slogan is that guns, independent of their applications or uses, are neutral. That is, guns in and of themselves are neither good nor bad. It would seem that there is an element of truth in this claim—After all, guns in and of themselves do not kill people. And until some person actually handles the gun, no one typically dies as a result of that gun. However, some critics note that the above slogan can be misleading if it is used to convey the claim that guns are neutral in the sense that they are no different from any other technologies or tools when it comes to violence.

Corlann Gee Bush (2006) has argued that gun technology, like all technologies, is biased in certain directions. She argues that certain features inherent in gun technology cause guns to be biased toward violence. To illustrate this bias, Bush appeals to an analogy from physics in which an atom that either loses or gains electrons through ionization becomes charged, or ''valenced'' in a certain direction. She notes that all technologies, including guns, are similarly valenced in that they tend to favor certain directions rather than others.

Bush concedes that devices other than guns can be used effectively to kill people. For example, a hammer, an ice pick, or even a certain kind of computer hardware device could each be used to kill someone. She argues, however, that guns are ''valenced toward violence'' in a way that other tools and technologies, which could also be used to kill people, are not. She points out that the mere presence of a gun in a particular situation raises the level of violence. Of course, an assailant could bludgeon someone to death by using a certain kind of computer hardware device. The assailant could also use a hammer to strike several blows to a person's head causing that person's death, or he could even stab someone to death with an ice pick. Although ice picks, hammers, and computer hardware devices *can* each be used to kill people, these objects are less likely to result in the unplanned or accidental death of an individual than would the presence of a gun in a similar situation. They are less likely to result in someone's death because of the respective purposes and functions of ice picks, hammers, and computing devices.

Note that in cases involving the presence of a computer device, an ice pick, or a hammer, an assailant must make physical contact with his victim and must then apply some measure

of physical force to carry out the murder. In the case involving a gun, on the contrary, the assailant is not required to make any physical contact at all. But perhaps more important, computer hardware devices, hammers, and ice picks are not charged or valenced toward killing someone in the same way guns are. The function of gun technology is such that it lends itself to violence and killing, by virtue of its intended purpose and design, even if a resultant death is not intended. So, if Bush is correct, technology is not neutral.

At this point, you might ask what, exactly, the preceding discussion about guns and about technologies being valenced has to do with our concern that computer technology might have embedded biases. Our purpose has been to show that all technologies, and by implication, computer technology, have embedded values and biases. Locating biases in software is important, and in Chapter 10 we examine some specific cases that illustrate gender bias in educational software and video games. Because Brey worries that some computer-ethics researchers may assume computer technology is inherently neutral, he proposes a method that causes us to question such an assumption. To employ his method, we need to locate what Brey calls ''embedded normative values'' in computer technology. Exposing such values inherent in various computer technologies is the first step of Brey's ''disclosive method of computer ethics.''

1.5.2 A "Disclosive" Method for Cyberethics

As noted earlier, Brey believes that the standard, or what he calls ''mainstream,'' applied-ethics methodology is not always adequate for identifying moral issues involving cyber-technology. Brey worries that using the standard model, we might fail to notice certain features embedded in the design of cybertechnology. He also worries that because the standard method of applied ethics tends to focus on known moral controversies, it fails to identify certain practices involving the use of cybertechnology that can also have moral import but that are not yet known. Brey refers to such practices as having ''morally opaque'' (or morally nontransparent) features, which he contrasts with ''morally transparent'' features.

According to Brey, morally controversial features that are transparent tend to be easily recognized as morally problematic. For example, many people are aware that the practice of placing closed circuit video surveillance cameras in undisclosed locations is controversial from a moral point of view. So, this would be an example of a morally transparent feature of technology. However, Brey notes that it is generally much more difficult to discern morally opaque features in technology. These features can be morally opaque for one of two reasons: Either they are unknown or they are known but perceived to be morally neutral.

Consider an example of each type of morally opaque (or morally nontransparent) feature. Computerized practices involving data mining (defined in Chapter 5) would be unknown to those who have never heard of the concept of data mining and who are unfamiliar with data-mining technology. However, this technology should not be assumed to be morally neutral merely because data mining techniques are unknown to nontechnical people, including many ethicists. Even if such techniques are opaque to many users, we will see that data mining practices raise certain moral issues pertaining to personal privacy.

Next consider an example of a morally opaque feature in which a technology is well known. Most Internet users are familiar with search-engine technology. What users might fail to realize, however, is that certain uses of search engines can be morally controversial with respect to personal privacy. Consequently, some features of search-engine technology

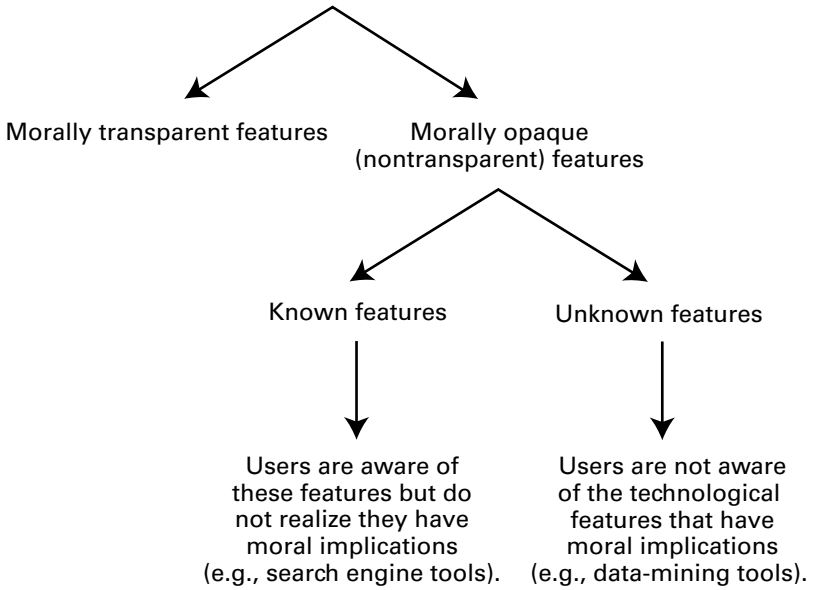

Figure 1-2 Embedded Technological Features Having Moral Implications

can be morally controversial in a sense that the controversies they raise are not obvious or transparent to many people, including those who are very familiar with and who use search-engine technology. So, although a well-known technology like search engines might appear to be morally neutral, a closer analysis of practices involving this technology will disclose concerns that also have moral implications.

Figure 1-2 illustrates some differences between morally opaque and morally transparent features.

Brey argues that an adequate methodology for computer ethics must first identify, or ''disclose,'' features that, without proper probing and analysis, would go unnoticed as having moral implications. Thus, an extremely important first step in Brey's ''disclosive method'' is to reveal moral values embedded in the various features and practices associated with cybertechnology itself.

1.5.3 An Interdisciplinary and Multilevel Method for Analyzing Cyberethics Issues

Brey's disclosive model is both *interdisciplinary* and *multilevel*. It is interdisciplinary because it requires the collaboration of computer scientists, philosophers, and social scientists, and it is multilevel because the method for conducting computer-ethics research requires three levels of analysis:

- disclosure level
- theoretical level
- application level

TABLE 1-3 Brey's Disclosive Model

Level	Disciplines Involved	Task/Function
Disclosure	Computer Science Social Science (optional)	Disclose embedded features in computer technology that have moral import
Theoretical	Philosophy	Test newly disclosed features against standard ethical theories
Application	Computer Science Philosophy Social Science	Apply standard or newly revised/formulated ethical theories to the issues

At the disclosure level, embedded moral values in the design of computer systems need to be disclosed. At this level, the technical expertise provided by computer scientists is critical, because this group of experts understands the details and nuances of computer technology in ways that philosophers and social scientists generally do not. Research at the disclosure level also often requires input from social scientists, however, who can evaluate aspects of system design from the perspective of human-interface requirements and expectations. After the embedded moral values have been disclosed, philosophers analyze the situation to determine whether the newly disclosed moral issues can be tested via existing ethical theories or whether additional theoretical analysis will be required. At the theoretical level, philosophers are capable of carrying out much of the required research. Finally, at the applications level, cooperation is needed among computer scientists, philosophers, and social scientists to complete the methodological process by applying ethical theory in deliberations about particular moral issues under consideration. In Chapter 2, we examine a range of ethical theories that can be used.

In the deliberations involved in applying ethical theory to a particular moral problem, one remaining methodological step must also be resolved. Jeroen van den Hoven (2000) has noted that methodological schemes must also address the ''problem of justification of moral judgments.'' For our purposes, key strategies of logical analysis are included in Chapter 3 to help us justify our conclusions about the judgments we make with respect to particular moral issues.

Table 1-3 describes the academic disciplines and the corresponding tasks and functions involved in Brey's disclosive model.

It is in the interdisciplinary spirit of the disclosive methodology proposed by Brey that we will examine the range of cyberethics issues described in Chapters 4–12.

▶ 1.6 A COMPREHENSIVE STRATEGY FOR APPROACHING CYBERETHICS ISSUES

The following methodological scheme, which expands on the original three-step scheme introduced in Section 1.4.2, is intended as a strategy to assist you in identifying and analyzing the specific cyberethics issues examined in this book. Note, however, that this procedure is *not* intended as a precise algorithm for resolving those issues in some definitive manner. Rather, its purpose is to guide you in the identification, analysis, and deliberation processes by summarizing key points that we have examined in Chapter 1:

Step 1. *Identify* a practice involving cybertechnology, or a feature of that technology, that is controversial from a moral perspective.

1a. Disclose any hidden or opaque features

1b. If the ethical issue is descriptive, assess the sociological implications for relevant social institutions and socio-demographic groups

1c. If ethical issue is also normative, determine whether there are any specific guidelines, that is, policies or ethical codes, that can help resolve the issue (for example, see the relevant professional codes of conduct described in Chapter 4 and Appendixes A–E).

1d. If the normative ethical issue cannot be resolved through the application of existing policies, codes of conduct, and so forth, go to Step 2.

Step 2. *Analyze* the ethical issue by clarifying concepts and situating it in a context.

2a. If a policy vacuums exists, go to Step 2b; otherwise go to Step 3.

2b. Clear up any conceptual muddles involving the policy vacuum and go to Step 3.

Step 3. *Deliberate* on the ethical issue. The deliberation process requires two stages:

3a. Apply one or more ethical theories (see Chapter 2) to the analysis of the moral issue, and then go to step 3b.

3b. Justify the position you reached by applying the rules for logical analysis and critical thinking (see Chapter 3).

Note that you are now in a position to carry out much of the work required in the first two steps of this methodological scheme. In order to satisfy the requirements in Step 1d, a step that is required in cases involving professional-ethics issues, you will need to consult the relevant sections of Chapter 4. Upon completing Chapter 2, you will be able to execute Step 3a, and after completing Chapter 3, you will be able to satisfy the requirements for Step 3b.

▶ 1.7 CHAPTER SUMMARY

In this introductory chapter, we defined several key terms, including *cyberethics* and *cybertechnology*, which are used throughout this textbook. We also briefly described four evolutionary phases of cyberethics, from its origins as a loosely configured and informal field concerned with ethical and social issues involving stand-alone (mainframe) computers to a more fully developed field that is currently concerned with ethical aspects of ubiquitous, networked computers. We then briefly considered whether any cyberethics issues are unique or special in a nontrivial sense. We next examined three different perspectives on cyberethics, showing how computer scientists, philosophers, and social scientists each tend to view the field and approach the issues that comprise it. Within that discussion, we also examined some ways in which embedded values and biases involving cybertechnology can be disclosed. Finally, we introduced a comprehensive methodological scheme that incorporates the expertise of computer scientists, philosophers, and social scientists who work in the field of cyberethics.

▶ REVIEW QUESTIONS

1. What, exactly, is *cyberethics*? How is it different from and similar to computer ethics and Internet ethics?
2. What is meant by the term *cybertechnology*? How is it similar to and different from computer technology?
3. Describe some ethical issues that arise in the case involving Verizon and the Recording Industry Association of America.
4. Describe some ethical concerns that arise in the Amy Boyer cyberstalking case.
5. Summarize the key aspects of each of the ''four phases'' we used to describe the evolution of cyberethics as a field of applied ethics.
6. Why does Walter Maner believe that some cyberethics issues are unique? Are any cyberethics issues unique or special in any philosophically interesting, or nontrivial, sense?
7. What alternative strategy does James Moor use to analyze the question whether cyberethics issues are unique?
8. Why does Moor believe that cybertechnology poses special problems for identifying and analyzing ethical issues?
9. Explain what Moor means by the expressions ''logical malleability,'' ''policy vacuum,'' and ''conceptual muddle.''
10. Identify the three distinct perspectives we used to approach cyberethics as a field of applied ethics.
11. Summarize the principal aspects of the perspective of cyberethics as a field of professional ethics.
12. Describe the principle aspects of the perspective of cyberethics as a field of philosophical ethics.
13. Summarize the key elements of the perspective of cyberethics as a field of descriptive ethics.
14. What is the difference between assertions or claims that are descriptive in nature and those that are normative? Provide an example of each.
15. Which criteria are used to distinguish normative ethical inquiries from those that are essentially descriptive?
16. What are the three elements of the standard, or ''mainstream,'' method for conducting applied-ethics research?
17. How is Philip Brey's ''disclosive method'' of computer ethics different from mainstream computer ethics?
18. How can Corlann Gee Bush's arguments about the nonneutrality of technology be used to support Brey's point about embedded values in cybertechnology?
19. What does Brey mean by ''morally opaque'' or ''morally nontransparent'' features embedded in computer technology?
20. In which ways is Brey's disclosive method both multilevel and interdisciplinary?

▶ DISCUSSION QUESTIONS

1. Analyze Don Gotterbarn's arguments for the claim that computer ethics is, at bottom, a field of applied ethics whose primary concern should be moral responsibility issues for computer professionals. Are his arguments convincing, or is his definition of the field too narrow, as some critics claim? How would you assess the impact of professional ethics issues in the overall scheme of cyberethics?
2. We briefly considered the question as to whether cyberethics issues are unique or special in any way. Luciano Floridi and J. W. Sanders (2002) have argued that certain issues raised by cybertechnology stretch and strain our ethical concepts in such a way that our traditional categories of ethics are no longer sufficient to handle these issues. And Hans Jonas (2006) has argued that modern technology has introduced ethical issues of such dramatic scale that our

traditional framework of ethics must be replaced with a new moral system. Assess Floridi's and Jonas's concerns, on the basis of what we have seen thus far about the kinds of moral issues generated by cybertechnology. Do we need a brand new framework of ethics?

3. Think of a controversial practice involving cybertechnology that has not yet been identified as an ethical issue, but which might eventually be recognized as one that has moral implications. Apply the first two steps of the three-step strategy that we developed in the concluding section of this chapter to your analysis of the issue/practice. Describe the conclusions you reached about this particular issue.
4. We identified three main perspectives from which cyberethics issues can be examined. Can you think of any additional perspectives from which cyberethics issues might also be analyzed? In addition to the Amy Boyer case, can you think of other cases involving cyberethics issues that would benefit from being analyzed from all three perspectives considered in Chapter 1? Explain.

▶ REFERENCES

Baase, Sara (2003). *A Gift of Fire: Social, Legal, and Ethical Issues in Computing.* 2nd ed. Upper Saddle River, NJ: Prentice Hall.

Brey, Philip (2004). "Disclosive Computer Ethics." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics.* 2nd ed. Sudbury, MA: Jones and Bartlett Publishers, pp. 55–66.

Brey, Philip (2005). "Freedom and Privacy in Ambient Intelligence," *Ethics and Information Technology*, Vol. 7, No. 3, pp. 157–166.

Buchanan, Elizabeth A. (2004). "Ethical Considerations for the Information Professions." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics.* 2nd ed. Sudbury, MA: Jones and Bartlett Publishers, pp. 613–624.

Bush, Corlann Gee (2006). "Women and the Assessment of Technology." In M. Winston and R. Edelbach, eds. *Society, Ethics, and Technology.* 3ed. Belmont, CA: Wadsworth, pp. 69–83.

Bynum, Terrell Ward (2004). "Ethics and the Information Revolution." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics.* 2nd ed. Sudbury, MA: Jones and Bartlett Publishers, pp. 13–29.

Floridi, Luciano, and J. W. Sanders (2002). "Mapping the Foundationalist Debate in Computer Ethics," *Ethics and Information Technology*, Vol. 4, No. 1, pp. 1–9.

Gotterbarn, Don (1995). "Computer Ethics: Responsibility Regained." In D. G. Johnson and H. Nissenbaum, eds. *Computing, Ethics, and Social Values.* Upper Saddle River, NJ: Prentice Hall.

Grodzinsky, Francis S., and Herman T. Tavani (2004). "Ethical Reflections on Cyberstalking." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics.* 2nd ed. Sudbury, MA: Jones and Bartlett, pp. 561–570.

Grodzinsky, Frances S., and Herman T. Tavani (2005). "P2P Networks and the *Verizon v. RIAA* Case," *Ethics and Information Technology*, Vol. 7, No. 4, pp. 243–250.

Huff, Chuck, and Thomas Finholt, eds. (1994). *Social Issues in Computing: Putting Computing in its Place.* New York: McGraw Hill.

Johnson, Deborah G. (2000). "The Future of Computer Ethics." In G. Cöllste, ed. *Ethics in the Age of Information Technology.* Linköping, Sweden: Centre for Applied Ethics, pp. 17–31.

Johnson, Deborah G. (2001). *Computer Ethics.* 3rd ed. Upper Saddle River, New Jersey: Prentice Hall.

Jonas, Hans (2006). "Technology and Responsibility: Reflections on the New Task of Ethics." In M. Winston and R. Edelbach, eds. *Society, Ethics, and Technology.* 3rd ed. Belmont, CA: Wadsworth, pp. 119–130.

Langford, Duncan, ed. (2000). *Internet Ethics.* New York: St. Martin's Press.

Maner, Walter (2004). "Unique Ethical Problems in Information Technology." In T. W. Bynum and S. Rogerson, eds. *Computer Ethics and Professional Responsibility.* Malden, MA: Blackwell, pp. 39–59.

Moor, James H. (2000). "What Is Computer Ethics?" In R. Baird, R. Ramsower, and S. Rosenbaum, eds. *Cyberethics: Social and Moral Issues in the Computer Age.* Amherst, NY: Prometheus Books, pp. 23–33.

Moor, James H. (2001). "The Future of Computer Ethics: You Ain't Seen Nothing Yet," *Ethics and Information Technology*, Vol. 3, No. 2, pp. 89–91.

Moor, James H. (2004). "Just Consequentialism and Computing." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics.* 2nd ed. Sudbury, MA: Jones and Bartlett, pp. 107–113.

Moor, James H. (2005). ''Should We Let Computers Get Under Our Skin?'' In R. Cavalier, ed. *The Impact of the Internet on Our Moral Lives.* Albany, NY: State University of New York Press, pp. 121–138.

Tavani, Herman T. (2001). ''The Current State of Computer Ethics as a Philosophical Field of Inquiry,'' *Ethics and Information Technology*, Vol. 3, No. 2, pp. 97–108.

Tavani, Herman T. (2002). ''The Uniqueness Debate in Computer Ethics: What Exactly Is at Issue, and Why Does it Matter?'' *Ethics and Information Technology*, Vol. 4, No. 1, pp. 37–54.

van den Hoven, Jeroen (2000). ''Computer Ethics and Moral Methodology.'' In R. Baird, R. Ramsower, and S. Rosenbaum, eds. *Cyberethics: Social and Moral Issues in the Computer Age.* Amherst, NY: Prometheus Books, pp. 80–94.

▶ FURTHER READINGS

Anderson, James G. and Kenneth W. Goodman (2001). *Ethics and Information Technology.* New York: Springer-Verlag.

Brennan, Linda L. and Victoria E. Johnson, eds. (2004). *Social, Ethical and Policy Implications of Information Technology.* Hershey, PA: Information Science Publishing.

Cavalier, Robert J., ed. (2005). *The Impact of the Internet on Our Moral Lives.* Albany, NY: State University of New York Press.

De George, Richard T. (2003). *Ethics of Information Technology and Business.* Malden, MA: Blackwell Publishers.

Gorniak-Kocikowska,Krystyna. (2004). ''The Computer Revolution and the Problem of Global Ethics.'' In T. W. Bynum and S. Rogerson, eds. *Computer Ethics and Professional Responsibility.* Malden, MA: Blackwell, pp. 319–326.

Gotterbarn, Don (2004). ''The Life Cycle of Cyber and Computing Ethics.'' In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics.* 2nd ed. Sudbury, MA: Jones and Bartlett Publishers, pp. 641–650.

Halbert, Terry, and Elaine Inguilli (2002). *Cyberethics.* Belmont, CA: Southwestern Thompson Learning.

Himma, Kenneth E. (2003). ''The Relationship Between the Uniqueness of Computer Ethics and its Independence as a Discipline in Applied Ethics,'' *Ethics and Information Technology*, Vol. 5, No. 4, pp. 225–237.

Huff, Chuck (2004). ''Unintentional Power and the Design of Computing Systems.'' In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics.* 2nd ed. Sudbury, MA: Jones and Bartlett Publishers, pp. 651–658.

Maner, Walter (2002). ''Heuristic Methods for Computer Ethics.'' In J. H. Moor and T. W. Bynum, eds. *Cyberphilosophy: The Intersection of Computing and Philosophy.* Malden, MA: Blackwell, pp. 243–269.

Mitcham, Carl, ed. (2005). *Encyclopedia of Science, Technology, and Ethics.* 4 Vols. New York: Macmillan.

Moore, Adam D. (2005). *Information Ethics: Privacy, Property, and Power.* Seattle, WA: University of Washington Press.

Spinello, Richard A. (2006). CyberEthics: *Morality and Law in Cyberspace.* 3rd ed. Sudbury, MA: Jones and Bartlett.

Tavani, Herman T., ed. (2006). *Ethics, Computing, and Genomics.* Sudbury, MA: Jones and Bartlett.

Winston, Morton, and Ralph Edelbach, eds. (2006) *Society, Ethics, and Technology.* 3rd ed. Belmont, CA: Wadsworth.

▶ ONLINE RESOURCES

Bibliography on Computing, Ethics, and Social Responsibility. http://cyberethics.cbi.msstate.edu/biblio/.

Developing on/off-lineComputer Ethics (Dolce). http://csethics.uis.edu/dolce/.

Heuristic Methods for Computer Ethics. http://csweb.cs.bgsu.edu/maner/heuristics/maner.pdf.

Research Center for Computing and Society. http://www.southernct.edu/organizations/rccs/.