CHAPTER

1

Introduction to Cyberethics: Concepts, Perspectives, and Methodological Frameworks

LEARNING OBJECTIVES

Upon completing this chapter, you will successfully be able to:

- Define *cybertechnology* and identify a wide range of technologies and devices that fall under that category,
- Define *cyberethics* and describe a cluster of moral, social, and legal issues that can be analyzed within that branch of applied ethics,
- Articulate key aspects of four distinct *phases* in the historical development and evolution of cybertechnology and cyberethics,
- Determine whether any of the ethical issues generated by cybertechnology are genuinely *unique* ethical issues, or whether they are simply new variations of traditional ethical issues,
- Differentiate among three distinct *applied ethics perspectives*—professional ethics, philosophical ethics, and sociological/descriptive ethics—that can be used to analyze the wide range of cyberethics issues examined in this book,
- Explain the components of a *comprehensive methodological framework* that we will use in our analysis of cyberethics issues in later chapters of this book.

Our primary objective in Chapter 1 is to introduce some foundational concepts and methodological frameworks that we will use to evaluate specific cyberethics issues examined in detail in subsequent chapters. We begin by reflecting on a scenario that briefly illustrates a cluster of ethical issues that arise in a recent controversy involving the use of cybertechnology.

► **SCENARIO 1–1:** Hacking into the Mobile Phones of Celebrities

In September 2014, one or more anonymous intruders hacked into the online accounts of the mobile phones of more than 100 celebrities, including actress Jennifer Lawrence and model Kate Upton. Nude photos of some of these celebrities were subsequently leaked to the Internet via the 4Chan Web site. The hacker(s) had allegedly broken into Apple Corporation's iCloud (a file-sharing service that enables users to store their data) gaining access to controversial pictures. Some of the celebrities whose accounts were hacked had previously deleted the photos on their physical devices and thus assumed that these pictures no longer existed.

Whereas some of the affected celebrities claimed that the nude photos of them were fake images, others admitted that the controversial pictures were authentic. Some of these celebrities threatened to bring legal action against anyone who posted nude photos of them on the Internet; for example, Jennifer Lawrence, through her spokesperson, warned that she would pursue criminal prosecution against those individuals.

In response to the intense media coverage generated by the hacking and leaking of the celebrities' photos, spokespersons for both Apple and the Federal Bureau of Investigation (FBI) announced that investigations into this incident were underway.[1] ■

This scenario raises a number of ethical, legal, and social issues affecting digital technology and cyberspace. One major concern involves privacy; in fact, Lawrence's attorney described the hacking incident as a "flagrant violation" of his client's privacy. Other issues that arise in this scenario involve property rights—for example, are the leaked photos in question solely the property of the celebrities (as in the case of the physical electronic devices these celebrities own)? Or does the fact that those photos also reside in the cloud alter their status as the sole property of an individual? Also, at issue in this scenario are questions concerning (cyber)security—how secure is the personal data stored on our devices or in a storage service space such as the cloud? Other aspects of this controversial incident can be analyzed from the perspective of (cyber)crime; for example, some have suggested that this kind of cyber intrusion is not simply a hacking incident, or merely an instance of online harassment, but is also a serious "sex crime."

The hacking scenario involving the celebrities' photos provides us with a context in which we can begin to think about a cluster of ethical issues—privacy, property, security, crime, harassment, and so forth—affecting the use of electronic devices, in particular, and cybertechnology in general. A number of alternative scenarios and examples could also have been used to illustrate many of the same moral and legal concerns that arise in connection with digital technology. In fact, examples abound. One has only to read a daily newspaper or view regular television news programs to be informed about controversial issues involving electronic devices and the Internet, including questions that pertain to property rights, privacy violations, security, anonymity, and crime. Ethical aspects of these and other issues are examined in the 12 chapters comprising this textbook. In the remainder of Chapter 1, however, we identify and examine some key foundational concepts and methodological frameworks that can better help us to analyze issues in cyberethics.

► 1.1 DEFINING KEY TERMS: CYBERETHICS AND CYBERTECHNOLOGY

Before we propose a definition of cyberethics, it is important to note that the field of cyberethics can be viewed as a branch of (applied) ethics. In Chapter 2, where we define ethics as "the study of morality," we provide a detailed account of what is meant by morality and a moral system, and we also focus on some important aspects of theoretical, as opposed to, applied ethics. For example, both ethical concepts and ethical theories are also examined in detail in that chapter. There, we also include a "Getting Started" section on how to engage in ethical reasoning in general, as well as reasoning in the case of some specific moral dilemmas. In Chapter 1, however, our main focus is on clarifying some key cyber and cyber-related terms that will be used throughout the remaining chapters of this textbook.

For our purpose, *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 communication devices, from stand-alone computers to connected, or networked, computing and communication technologies. These technologies include, but need not be limited to, devices such as "smart" phones, iPods, (electronic) tablets, personal computers (desktops and laptops), and large 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 other hand, 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 U.S. 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 is thus available to anyone. The Internet, which should be differentiated from the World Wide Web, includes several applications. The Web, based on Hypertext Transfer Protocol (HTTP), is one application; other applications include File Transfer Protocol (FTP), Telnet, and e-mail. Because many users navigate 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 is 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 and communication systems, from stand-alone computers to privately owned networks and to the Internet itself. "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 technologies (see, e.g., Barger 2008; Johnson 2010). Others use the expression "information ethics" (e.g., Capurro 2007) to refer to a cluster of ethical concerns regarding the flow of information that is either enhanced or restricted by computer technology.[2] And because of concerns about ethical issues involving the Internet in particular, some have also used the term "Internet ethics" (see, e.g., Langford 2000). As we shall see, however, there are some disadvantages to using each of these expressions, especially insofar as each fails to capture the wide range of moral issues involving cybertechnology.[3]

For our purposes, "cyberethics" is more appropriate and more accurate than "computer 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 communication 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 affecting computer/information technology (IT) professionals. Although these issues are very important and are examined in detail in Chapter 4 as well as in relevant sections of Chapters 6 and 12, we should note that the field of cyberethics is not limited to an analysis of moral issues that affect only professionals.

"Cyberethics" is also more accurate, for our purposes, than "information ethics." For one thing, the latter expression is ambiguous because it can mean a specific methodological framework *Information Ethics (IE)* for analyzing issues in cyberethics (Floridi 2007).[4] Also, it can connote a cluster of ethical issues of particular interest to professionals in the fields of library science and information science (Buchanan and Henderson 2009). In the latter sense, "information ethics" refers to ethical concerns affecting the free flow of, and unfettered access to, information, which include issues such as library censorship and intellectual freedom. (These issues are examined in Chapter 9.) Our analysis of cyberethics issues in this text, however, is not limited to controversies generally considered under the heading "information ethics."

We will also see why "cyberethics" is preferable to "Internet ethics." For one thing, the ethical issues examined in this textbook are not limited to the Internet; they also include privately owned computer networks and interconnected communication technologies—that is, technologies that we refer to collectively as cybertechnology. Although most of the issues considered under the heading cyberethics pertain to the Internet or the Web, some issues examined in this textbook do not involve networks 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 cybertechnology for gender and race need not involve networked computers and devices. In light of the wide range of moral issues examined in this book—ethical issues that cut across the spectrum of devices and communication systems (comprising cybertechnology), from stand-alone computers to networked systems—the term "cyberethics" is more comprehensive, and thus more appropriate, than "Internet ethics."[5]

Finally, we should note that some issues in the emerging fields of "agent ethics," "bot ethics," "robo-ethics," or what Wallach and Allen (2009) call "machine ethics" overlap with a cluster of concerns examined under the heading of cyberethics. Wallach and Allen define machine ethics as a field that expands upon traditional computer ethics because it shifts the main area of focus away from "what people do with computers to questions about what machines do by themselves." It also focuses on questions having to do with whether computers can be autonomous agents capable of making good moral decisions. Research in machine ethics overlaps with the work of interdisciplinary researchers in the field of artificial intelligence (AI).[6] We examine some aspects of this emerging field (or subfield of cyberethics) in Chapters 11 and 12.

► 1.2 THE CYBERETHICS EVOLUTION: FOUR DEVELOPMENTAL PHASES IN CYBERTECHNOLOGY

In describing the key evolutionary phases of cybertechnology and cyberethics, we begin by noting that the meaning of "computer" has evolved significantly since the 1940s. If you were to look up the meaning of that word in a dictionary written before World War II, you would most likely discover that a computer was defined as a person who calculated numbers. In the time period immediately following World War II, the term "computer" came to be identified with a (calculating) machine as opposed to a person (who calculated).[7] By the 1980s, however, computers had shrunk in size considerably and they were beginning to be understood more in terms of desktop machines (that manipulated symbols as well as numbers), or as a new kind of medium for communication, rather than simply as machines that crunch numbers. As computers became increasingly connected to one another, they came to be associated with metaphors such as the "information superhighway" and cyberspace; today, many ordinary users tend to think about computers in terms of various Internet- and Web-based applications made possible by cybertechnology.

In response to some social and ethical issues that were anticipated in connection with the use of electronic computers, the field that we now call cyberethics had its informal and humble beginnings in the late 1940s. It is interesting to note that during this period—when ENIAC (Electronic Numerical Integrator and Computer), the first electronic computer, developed at the University of Pennsylvania, became operational in 1946—some analysts confidently predicted that no more than five or six computers would ever need to be built. It is also interesting to point out that during this same period, a few insightful thinkers had already begun to describe some social and ethical concerns that would likely arise in connection with computing and cybertechnology.[8] Although still a relatively young academic field, cyberethics has now matured to a point where several articles about its historical development have appeared in books and scholarly journals. For our purposes, the evolution of cyberethics can be summarized in four distinct *technological phases*.[9]

Phase 1 (1950s and 1960s): Large (Stand-Alone) Mainframe Computers

In *Phase 1*, computing technology consisted mainly of huge mainframe computers, such as ENIAC, 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). The following kinds of questions were introduced in Phase 1: Can machines think? If so, should we invent 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 threats 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 would 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, which was funded by an agency in the U.S. Defense Department—began during this phase, in the 1960s.

Phase 2 (1970s and 1980s): Minicomputers and Privately Owned Networks

In *Phase 2*, computing machines and communication 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 1.1.1), and information could readily be exchanged between and among databases accessible to networked computers.

Ethical issues associated with this phase of computing included concerns about personal privacy, intellectual property (IP), and computer crime. Privacy concerns, which had emerged during Phase 1 because of worries about the amount of personal information that could be collected by government agencies and stored in a centralized government-owned database, were exacerbated because electronic records containing personal and confidential information could now also easily be exchanged between two or more commercial databases in the private sector. Concerns affecting IP and proprietary information also emerged during this phase because personal (desktop) computers could be used to duplicate proprietary software programs. And concerns associated with 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.

Phase 3 (1990–Present): The Internet and World Wide Web

During *Phase 3*, 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 in the 1990s. The proliferation of Internet- and Web-based technologies has contributed to some additional ethical concerns involving computing technology; for example, issues of free speech, anonymity, jurisdiction, and trust have been hotly disputed during this phase. Should Internet users be free to post any messages they wish on publicly accessible Web sites or even on their own personal Web pages—in other words, is that a "right" that is protected by free speech or freedom of expression? Should users be permitted to post anonymous messages on Web pages or even be allowed to navigate the Web anonymously or under the cover of a pseudonym?

Issues of jurisdiction also arose because there are no clear national or geographical boundaries in cyberspace; if a crime occurs on the Internet, it is not always clear where—that is, in which legal jurisdiction—it took place and thus it is unclear where it should be prosecuted. And as e-commerce emerged during this phase, potential consumers initially had concerns about trusting online businesses with their financial and personal information. Other ethical and social concerns that arose during Phase 3 include disputes about the public vs. private aspects of personal information that has become increasingly available on the Internet. Concerns of this type have been exacerbated by the amount of personal information included on social networking sites, such as Facebook and Twitter, and on other kinds of interactive Web-based forums made possible by "Web 2.0" technology (described in Chapter 11).

We should note that during Phase 3, both the interfaces used to interact with computer technology and the devices used to "house" it were still much the same as in Phases 1 and 2. A computer was still essentially a "box," that is, a CPU, with one or more peripheral devices, such as a video screen, keyboard, and mouse, serving as interfaces 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, however, 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, Moor (2005) notes that computing devices will soon be a part of our clothing and even our bodies. This brings us to Phase 4.

Phase 4 (Present–Near Future): Converging and Emerging Technologies

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 aspects of technological convergence beginning in Phase 2, where the integration of computing and communication devices resulted in privately owned networked systems, as we noted previously. And in Phase 3, the Internet era, we briefly described the convergence of text, video, and sound technologies on the Web, and we noted how the computer began to be viewed much more as a new kind of medium than as a conventional type of machine. The convergence of information technology and biotechnology in recent years has resulted in the emerging fields of bioinformatics and computational genomics; this has also caused some analysts to question whether computers of the future will still be silicon based or whether some may also possibly be made of biological materials. Additionally, biochip implant technology, which has been enhanced by developments in AI research (described in Chapter 11), 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.

Today, computers are also ubiquitous or pervasive; that is, they are "everywhere" and they permeate both our workplace and our recreational environments. Many of the objects that we encounter in these environments are also beginning to exhibit what Brey (2005) and others call "ambient intelligence," which enables "smart objects" to be connected to one another via

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 the ARPANET; desktop computers interconnected via privately owned networks; not yet widely accessible to the general public	Issues from Phase 1 plus concerns involving intellectual property and software piracy, computer crime, and communications privacy
3	1990s–present	Internet, World Wide Web, and early "Web 2.0" applications, environments, and forums; became accessible to ordinary people	Issues from Phases 1 and 2 plus concerns about free speech, anonymity, legal jurisdiction, behavioral norms in virtual communities
4	Present to near future	Convergence of information and communications technologies with nanotechnology and biotechnology, in addition to developments in emerging technologies such as AmI, augmented reality, and 3D printing	Issues from Phases 1–3 plus concerns about artificial electronic agents ("bots") with decision-making capabilities, AI-induced bionic chip implants, nanocomputing, pervasive computing, Big Data, IoT, etc.

wireless technology. Some consider radio-frequency identification (RFID) technology (described in detail in Chapter 5) to be the first step in what is now referred to as the Internet of Things (IoT), as well as *pervasive* or *ubiquitous computing* (described in detail in Chapter 12).

What other kinds of technological changes should we anticipate as research and development continue in Phase 4? For one thing, computing devices will likely continue to become more and more indistinguishable from many kinds of noncomputing devices. For another thing, a computer may no longer typically be conceived of as a distinct device or object with which users interact via an explicit interface such as a keyboard, mouse, and video display. We are now beginning to conceive of computers and cybertechnology in drastically different ways. Consider also that computers are becoming less visible—as computers and electronic devices continue to be miniaturized and integrated/embedded in objects, they are also beginning to "disappear" or to become "invisible" as distinct entities.

Many analysts predict that computers and other electronic devices will become increasingly smaller in size, ultimately achieving the nanoscale. (We examine some ethical implications of nanotechnology and nanocomputing in Chapter 12.) Many also predict that aspects of nanotechnology, biotechnology, and information technology will continue to converge. However, we will not speculate any further in this chapter about either the future of cybertechnology or the future of cyberethics. The purpose of our brief description of the four phases of cybertechnology mentioned here is to provide a historical context for understanding the origin and evolution of at least some of the ethical concerns affecting cybertechnology that we will examine in this book.

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 Scenario 1–1, in the chapter's opening section. Have any new ethical issues been introduced in the hacking incident described in that scenario? Or are the issues that arise here merely examples of existing ethical issues that may have been exacerbated in some sense by new technologies, including new storage systems to archive personal data? Also, consider some factors having to do with *scope* and *scale*: The hacked photos of the celebrities can be seen by millions of people around the world, as opposed to previous cases where one might have to go to an "adult" store to acquire copies of the nude photos. Also, consider that harassment-related activities of the kind described in Scenario 1–1 can now occur on a scale or order of magnitude that could not have been realized in the pre-Internet era.

But do these factors support the claim that cybertechnology has introduced some new and unique ethical issues? Maner (2004) argues that computer use has generated a series of ethical issues that (i) did not exist before the advent of computing and (ii) could not have existed if computer technology had not been invented.[10] 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 1–2:** Developing the Code for a Computerized Weapon System

Sally Bright, a recent graduate from Technical University, has accepted a position as a software engineer for a company called Cyber Defense, Inc. This company has a contract with the U.S. Defense Department to develop and deliver applications for the U.S. military. When Sally reports to work on her first day, she is assigned to a controversial project that is developing the software for a computer system designed to deliver chemical weapons to and from remote locations. Sally is conflicted about whether she can, given her personal values, agree to work on this kind of weapon delivery system, which would not have been possible without computer technology. ■

Is the conflict that Sally faces in this particular scenario one that is new or unique because of computers and cybertechnology? One might argue that the ethical concerns surrounding Sally's choices are unique because they never would have arisen had it not been for the invention of computer technology. In one sense, it is true that ethical concerns having to do with whether or not one should participate in developing a certain kind of computer system did not exist before the advent of computing technology. However, it is true only in a trivial sense. Consider that long before computing technologies were available, engineers were confronted 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, for example, 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 scenario? Have any new or unique ethical issues, in a nontrivial sense of "unique," been generated here? Based on our brief analysis of this scenario, there does not seem to be sufficient evidence to substantiate the claim that one or more new ethical issues have been introduced.

▶ **SCENARIO 1–3:** Digital Piracy

Harry Flick is an undergraduate student at Pleasantville State College. In many ways, Harry's interests are similar to those of typical students who attend his college. But Harry is also very fond of classic movies, especially films that were made before 1950. DVD copies of these movies are difficult to find; those that are available tend to be expensive to purchase, and very few are available for loan at libraries. One day, Harry discovers a Web site that has several classic films (in digital form) freely available for downloading. Since the movies are still protected by copyright, however, Harry has some concerns about whether it would be permissible for him to download any of these films (even if only for private use). ■

Is Harry's ethical conflict one that is unique to computers and cybertechnology? Are the ethical issues surrounding Harry's situation new and thus unique to cybertechnology, because the practice of downloading digital media from the Internet—a practice that many in the movie and recording industries call "digital piracy"—would not have been possible if computer technology had not been invented in the first place? If so, this claim would, once again, seem to 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" audio cassette tapes 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 audio cassette tapes are, at bottom, the same issues underlying the pirating of digital media. They arise in each case because, fundamentally, the behavior associated with unauthorized copying raises moral concerns about property, fairness, rights, and so forth. So, as in Scenario 1–2, there seems to be insufficient evidence to suggest that the ethical issues associated with digital piracy are either new or unique in some nontrivial sense.

1.3.1 Distinguishing between Unique Technological Features and Unique Ethical Issues

Based on 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, and so forth 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 that technology 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. The fallacy can be expressed in the following way:

PREMISE 1. Cybertechnology has some unique technological features.

PREMISE 2. Cybertechnology has generated some ethical concerns.

CONCLUSION. At least some ethical concerns generated by cybertechnology must be unique ethical concerns.

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 generated by that technology.[11]

1.3.2 An Alternative Strategy for Analyzing the Debate about the Uniqueness of Cyberethics Issues

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 warrant special consideration from an ethical perspective. But what, exactly, is so different about issues involving computers and cybertechnology that make them deserving of special moral consideration? Moor (2007) 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."[12] 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 to resolve a policy vacuum when it is discovered? Initially, a solution to this problem might seem quite simple and straightforward. 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.

1.3.3 A Policy Vacuum in Duplicating Computer Software

A critical 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 run on computers. Although there were IP laws in place, it had not been determined that software was or should be protected by 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 herself? Could she share it with a friend? Could she 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 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 controversies surrounding the original Napster Web site and the Recording Industry Association of America (RIAA), in the late 1990s, regarding the free exchange of music over the Internet. Proponents on both sides of this 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 (digitized music in the form of MP3 files) being exchanged between Internet users and the technology (P2P systems) that facilitated this exchange. Although cybertechnology has made it possible to exchange MP3 files, there is still debate, and arguably a great deal of confusion as well, about whether doing so should necessarily be illegal. Until the conceptual confusions or muddles underlying arguments used in the Napster vs. RIAA case in particular, and about the nature of P2P file-sharing systems in general, are resolved, it is difficult to frame an adequate policy regarding the exchange of MP3 files in P2P transactions.

How 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 associated with cybertechnology—that is, issues involving privacy, IP, 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, or practical 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. Recall that at the heart of this dispute is the question: should proprietary information, in a digital format known as MP3 files, be allowed to be exchanged freely over the Internet? 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 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, an important consideration for an ethical policy is that it protects the rights of individuals—in this case, the rights of those 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 our analysis of the dispute over the exchange of MP3 files on the Internet (in the Napster case), the application of two different ethical theories yielded 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 sociological/descriptive ethics. Gaining a clearer understanding of what is meant by each perspective 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 and IT professionals. Among the cyberethics issues considered from this perspective are those having to do with the computer/IT professional's role in designing, developing, and maintaining computer hardware and software systems. For example, 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 principal focus of analysis is on issues of moral responsibility that affect individuals as members of these *professions*. By analogy, they would go on to argue that the same rationale should apply to the field of cyberethics—that is, the primary, and possibly even exclusive, focus of cyberethics should be on issues of moral responsibility that affect computer/IT professionals. Gotterbarn (1995) can be interpreted as defending a version of this position when he asserts

> The only way to make sense of 'Computer Ethics' is to narrow its focus to those actions that are within the control of the individual *moral* computer professional.[13] [Italics Gotterbarn]

So, in this passage, Gotterbarn suggests 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 Gotterbarn uses to defend his argument are instructive. He 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 field of computer science. However, some of those practitioners, as well as many philosophers and social scientists, believe that Gotterbarn's conception of computer ethics as simply a field of professional ethics is 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 a broader model is needed. For example, Buchanan (2004), in describing the importance of analyzing ethical issues in the "information professions," suggests that some nonprofessional ethics issues must also be examined because of the significant impact they have on noninformation professionals, including ordinary computer users. Consider that these issues can also affect people who have never used a computer.

Of course, Buchanan's category of "information 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 computer ethics as a field limited to the study of ethical issues affecting computer professionals seemed plausible. Now, computers are virtually everywhere, and the ethical issues generated by certain uses of computers and cybertechnology affect virtually everyone, professional and nonprofessional alike.

Despite the critiques leveled against Gotterbarn's conception of the field, his position may turn out to be the most plausible of the three models we consider. Because of the social impact that computer and Internet technologies have had during the past three decades, we have tended to identify many of the ethical issues associated with these technologies, especially concerns affecting privacy and IP, as computer ethics issues. But Johnson (2000) believes that in the future, computer-related ethical issues, such as privacy and property (that 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." 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 turn out to be the correct one in the long term.

Applying the Professional Ethics Model to Specific Scenarios

It is fairly easy to see how the professional ethics model can be used to analyze issues involving professional responsibility that directly impact computer/IT professionals. For example, issues concerned with the development and implementation of critical software would fit closely with the professional model. But can that model be extended to include cases that may only affect computer professionals indirectly? Consider again Scenario 1–1, where celebrities' photos were hacked and subsequently leaked to the Internet. While the unauthorized break-ins into one's property and the posting/displaying nude photos of celebrities are both illegal and immoral acts, are they also examples of a computer ethics issue that affects computer/IT professionals and the computer profession? Arguably, computer corporations such as Apple are responsible for securing the data that resides in their storage systems, such as the iCloud, from cyberattacks of this kind. One could also argue that if the software engineers employed by these corporations had written more effective code, the hackers might have been prevented from accessing the controversial photos. So it would seem that there are at least some indirect ways that the professional ethics perspective can be brought to bear on this scenario. Of course, there are many other ethically controversial aspects of Scenario 1–1 that do not pertain directly to computer professionals and software engineers.

Many of the ethical issues discussed in this book have implications for computer/IT 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 likely also want to assess some of the indirect implications that issues examined in Chapters 5 through 12 also 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? Since 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 of cyberethics as a branch of philosophical ethics, consider James Moor's classic definition of the field. According to Moor (2007), cyberethics, or what he calls "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.[14]

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 the impact of that technology for computer professionals. Secondly, this definition challenges us to reflect on the social impact of cybertechnology in a way that also 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 aren't 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 could respond to Gotterbarn's point by noting 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

Brey (2004) notes that 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.[15]

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 digital piracy. 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 digital piracy, we saw that the concept of piracy could be analyzed in terms of moral issues involving theft and IP 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 digital piracy 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 Specific Scenarios

To see how the philosophical ethics perspective of cyberethics can help us to analyze a cluster of moral issues affecting cybertechnology, we once again revisit Scenario 1–1. In applying the philosophical ethics model to this scenario, our first task is to identify one or more moral issues that arise in that context; we have already seen that this scenario illustrates a wide range of ethical issues. For example, we saw that the range of ethical issues include privacy and anonymity, security and crime, property rights and free speech, and so forth.

We can now ask, what kinds of policy vacuums and conceptual muddles, if any, also arise in this scenario? For one thing, questions affecting property rights here might seem a bit stretched and strained and thus challenge some of our received notions affecting property. However, policy vacuums concerning IP in the digital era are by no means new. For example, we noted earlier that the original Napster scenario introduced controversies with respect to sharing copyrighted information, in the form of proprietary MP3 files, online. Scenario 1–1, however, introduces a property-related issue that goes beyond that kind of concern. Here, we have a question about one's claim to the sole ownership of a digital image that resides in a company's storage facility, that is, in addition to, or in place of, residing on a person's electronic device.

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

The two perspectives on cyberethics that we have examined thus far—professional ethics and philosophical ethics—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 is, or aims to be, nonevaluative in approach; typically, it describes particular moral systems and sometimes also reports how members of various groups and cultures view particular moral issues. This kind of analysis of ethical and social issues is often used by sociologists and social scientists—hence, our use of the expression "sociological/descriptive perspective" to analyze this methodological framework.

Descriptive vs. Normative Inquiries

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 specific technology on a particular community or social group. 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 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 sociological/descriptive ethics.

▶ **SCENARIO 1–4:** The Impact of Technology X on the Pleasantville Community

AEC Corporation, a company that employs 8,000 workers in Pleasantville, has decided to purchase and implement a new kind of digital technology, Technology X. The implementation of Technology X will likely have a significant impact for AEC's employees in particular, as well as for Pleasantville in general. It is estimated that 3,000 jobs at AEC will be eliminated when the new technology is implemented during the next six months. ■

Does the decision to implement Technology X pose a normative ethical problem for the AEC Corporation, as well as for Pleasantville? If we analyze the impact that Technology X has with respect to the number of jobs that are gained or lost, our investigation is essentially descriptive in nature. In reporting this phenomenon, we are simply describing or stating what *is/is not* at issue in this case. If, however, we argue that AEC either should or should not implement this new technology, then we make a claim that is normative (i.e., a claim about what *ought/ought not* to be the case). For example, one might argue that the new technology should not be implemented because it would displace workers and thus possibly violate certain contractual obligations that may exist between AEC and its employees. Alternatively, one might argue that implementing Technology X would be acceptable provided that certain factors are taken into consideration in determining which workers would lose their jobs. For example, suppose that in the process of eliminating jobs, older workers and minority employees would stand to be disproportionately affected. In this case, critics might argue that a fairer system should be used.

Our initial account of the impact of Technology X's implementation for Pleasantville simply reported some descriptive information about the number of jobs that would likely be lost by employees at AEC Corporation, which has sociological implications. As our analysis of this scenario continued, however, we did much more than merely describe what the impact was; we also evaluated the impact for AEC's employees in terms of what we believed *ought* to have been done. In doing so, we shifted from an analysis based on claims that were merely descriptive to an analysis in which some claims were also normative.

Some Benefits of Using the Sociological/Descriptive Approach to Analyze Cyberethics Issues

Why is the examination of cyberethics issues from the sociological/descriptive ethics perspective useful? Huff and Finholt (1994) suggest that focusing on descriptive aspects of social issues can help us to better understand many of the normative features and implications. In other words, when we understand the descriptive features of the social effects of a particular technology, the normative ethical questions become clearer. So Huff and Finholt believe that analyzing the social impact of cybertechnology from a sociological/descriptive perspective can better prepare us for our subsequent analysis of practical ethical issues affecting our system of policies and laws.

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 sociological/descriptive ethics, we can also better examine the impact that cybertechnology has on our understanding of concepts such as community and individuality. We can ask, for instance, whether certain developments in social networking technologies used in Twitter and Facebook 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, or perhaps a similar ideology, irrespective of geographical limitations? Is national identity something that is, or may soon become, anachronistic? While 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 Chapters 10 and 11, where we examine the impact of cybertechnology on sociodemographic groups and on some of our social and political institutions.

Applying the Sociological/Descriptive Ethics Approach to Specific Scenarios

Consider how someone approaching cyberethics issues from the perspective of sociological/descriptive ethics might analyze the scenario involving the hacked photos of celebrities described in Scenario 1–1. In this case, the focus might be on gathering sociodemographic and socioeconomic data pertaining to the kinds of individuals who are likely to hack into a celebrity's cell phone or electronic device. For example, some social scientists might consider the income and educational levels of hackers, as compared to individuals who engage in alternative kinds of online activities or who do not use the Internet at all. Others might further inquire into why some individuals seem to display little-to-no concern about posting nude photos of people that could be viewed, potentially at least, by millions of people. Still others engaged in research from the point of view of sociological/descriptive ethics might inquire into whether there has been an increase in the number of hacking incidents in recent years. And if the answer to this question is "yes," the researcher might next question whether such an increase is linked to the widespread availability of hacking tools that are now available on the Internet.

Also, the researcher might consider whether certain groups in the population are now more at risk than others with respect to being hacked. That researcher could further inquire whether there are any statistical patterns to suggest that female celebrities are more likely to be hacked than are individuals in other groups. The researcher could also ask if women in general are typically more vulnerable than men to the kinds of harassment associated with this form of online behavior.

Also, a researcher approaching this scenario from the sociological/descriptive ethics perspective might set out to determine whether an individual who never would have thought of physically harassing a person in geographical space might now be inclined to do so 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 hacker realizes that he or she can harass a person on the Internet under the cloak of relative anonymity/pseudonymity contributed to the increase in harassment online? These are a few of the kinds of questions that could be examined from the sociological/descriptive perspective of cyberethics.

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

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
Sociological/descriptive	Sociology/behavioral sciences	Impact of cybertechnology on governmental/financial/educational institutions and sociodemographic groups

In Chapters 4–12, we examine specific cyberethics questions from the vantage points of our three perspectives. Issues considered from the perspective of professional ethics are examined in Chapters 4 and 12. Cyberethics issues considered from the perspective of philosophical ethics, such as those involving privacy, security, IP, and free speech, are examined in Chapters 5–9. And several of the issues considered in Chapters 10 and 11 are examined from the perspective of sociological/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, that is, where a researcher must (i) identify an ethical problem, (ii) describe and analyze the problem in conceptual and factual terms, and (iii) apply ethical theories and principles in the deliberative process. We also saw that Moor argued that the conventional model was not adequate for an analysis of at least some cyberethics issues. Moor believed that additional steps, which address 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, critics, including some feminists, 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 account for the bias embedded in that particular technological system.

1.5.1 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 cybertechnology. Brey worries that using the standard model we might fail to notice certain features embedded in the design of cybertechnology. He also worries about the standard method of applied ethics because it tends to focus on known moral controversies, and because it fails to identify certain practices involving the use of cybertechnology that 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. Brey notes that it is, however, 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.[16]

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 some ethicists as well. Even if such techniques are opaque to many users, 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 recognize, however, is that certain uses of search engines can be morally controversial with respect to personal privacy. Consequently, one of the features of search engine technology can be morally controversial in a sense that it is not obvious or transparent to many people, including those who are very familiar with and who use search engine technology. So, while a well-known technology, such as search engine programs, might appear to be morally neutral, a closer analysis of practices involving this technology will disclose that it has moral implications.

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

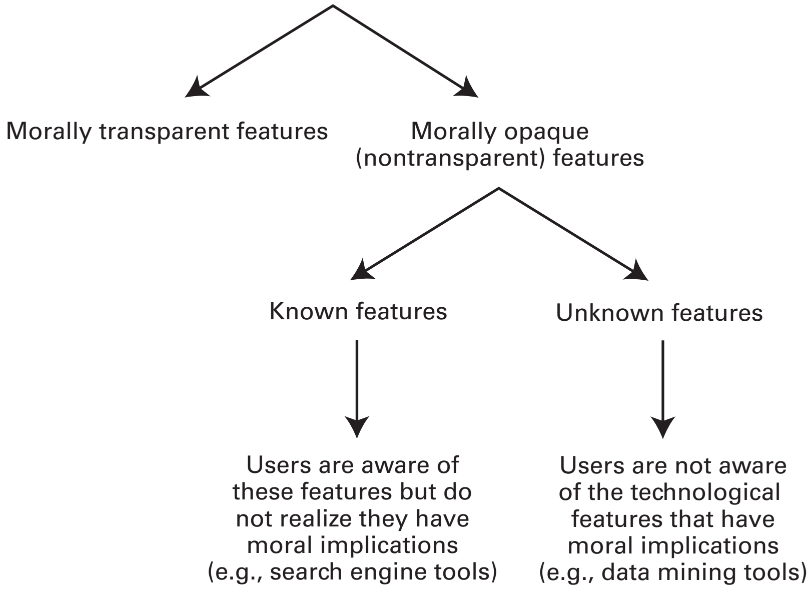
Morally transparent features
Morally opaque (nontransparent) features
Known features
Unknown features
Users are aware of these features but do not realize they have moral implications (e.g., search engine tools)
Users are not aware of the technological features that have moral implications (e.g., data mining tools)

Figure 1-1 Embedded technological features having moral implications.

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.

1.5.2 An Interdisciplinary and Multilevel Method for Analyzing Cyberethics Issues

Brey's disclosive model is *interdisciplinary* because it requires that computer scientists, philosophers, and social scientists collaborate. It is also *multilevel* because conducting computer ethics research requires three levels of analysis:

- Disclosure level
- Theoretical level
- Application level

First of all, the moral values embedded in the design of computer systems must be disclosed. To do this, we need computer scientists because they understand computer technology much better than philosophers and social scientists do. However, social scientists are also needed to evaluate system design and make it more user-friendly. Then philosophers can determine whether existing ethical theories are adequate to test the newly disclosed moral issues or whether more theory is needed. Finally, computer scientists, philosophers, and social scientists must cooperate by applying ethical theory in deliberations about moral issues.[17] 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 also needs to be resolved. Van den Hoven (2000) has noted that methodological schemes must also address the "problem of justification of moral judgments." For our purposes, we use the strategies of logical analysis included in Chapter 3 to justify the moral theories we apply to particular issues.

Table 1-3 summarizes the three levels, academic disciplines, and 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 Chapter 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

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

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.** Assess any descriptive components of the ethical issue via the sociological implications it has for relevant social institutions and sociodemographic groups.
- **1c.** In analyzing the normative elements of that issue, determine whether there are any specific guidelines, that is, social policies or ethical codes, that can help resolve the issue (e.g., see the relevant professional codes of conduct described in Chapter 4 as well as in Appendices A–E, available at www.wiley.com/college/tavani).
- **1d.** If the normative ethical issue cannot be resolved through the application of existing policies, codes of conduct, and so on, 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 evaluating it via the standards and criteria for successful logic argumentation (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*, 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 today concerned with ethical aspects of ubiquitous, networked computers and devices. 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 affecting cybertechnology can be disclosed and thus made explicit. 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, information ethics, and Internet ethics?

2. What is meant by the term *cybertechnology*? How is it similar to and different from computer technology?

3. Describe in detail each of the "four phases" involving the evolution of cybertechnology. What are the key technological developments in each phase?

4. Describe in detail each of the four phases comprising the development of cyberethics as a field of applied ethics. What are the key ethical issues that arise in each phase?

5. Why does Walter Maner believe that at least some cyberethics issues are unique? What arguments does he provide to support his view?

6. Why is it important to distinguish between unique technological features and unique ethical issues when evaluating the question, Are cyberethics issues unique?

7. What alternative strategy does James Moor use to analyze the question whether cyberethics issues are unique ethical issues?

8. Why does Moor believe that cybertechnology poses special problems for identifying and analyzing ethical issues?

9. Explain what Moor means by the expression "logical malleability," and why he believes that this technological feature of computers is significant.

10. What does Moor mean by the phrase "policy vacuum," and what role do these vacuums play in understanding cyberethics?

11. Explain what Moor means by a "conceptual muddle". How can these muddles sometimes complicate matters when trying to resolve policy vacuums?

12. Summarize the principal aspects of the perspective of cyberethics as a field of *professional* ethics.

13. Describe the principal aspects of the perspective of cyberethics as a field of *philosophical* ethics.

14. Summarize the key elements of the perspective of cyberethics as a field of *sociological/descriptive* ethics.

15. Describe the kinds of criteria 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 what Brey calls "mainstream computer ethics"?

18. What does Brey mean by "morally opaque" or "morally nontransparent" features embedded in computer technology?

19. In which ways is Brey's disclosive method "multilevel"? Briefly describe each level in his methodology.

20. In which ways is that method also "multidisciplinary" or interdisciplinary? Which disciplines does it take into consideration?

▶ DISCUSSION QUESTIONS

21. Assess Don Gotterbarn's arguments for the claim that computer ethics is, at bottom, a field whose primary concern should focus on moral responsibility issues for computer professionals. Do you agree with his position?

22. Think of a controversial issue or 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 Brey's "disclosive method" to see whether you can isolate any embedded values or biases affecting that practice. Also, be sure to separate any "morally opaque features" from those that are "morally transparent" (or nonopaque).

23. 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?

24. Identify a current ethical issue involving the use of a recent or emerging technology. Apply the three-step process in the "comprehensive framework" (or strategy for Approaching Moral Issues in Cybertechnology) that we articulated in Section 1.6.

Scenarios for Analysis

1. We briefly considered the question whether some cyberethics issues are new or unique ethical issues. In the following scenario, which could be titled "Contesting the Ownership of a Twitter Account," (i) identify the ethical issues that arise and (ii) determine whether any of them are unique to cybertechnology.

Noah Kravitz was employed by PhoneDog Media, a mobile phone company, for nearly four years. PhoneDog had two divisions: an e-commerce site (phonedog.com) that sold mobile phones and a blog that enabled customers to interact with the company. Kravitz created a blog on Twitter (called Phonedog_Noah) while employed at PhoneDog, and his blog attracted 17,000 followers by the time he left the company in October 2010. However, Kravitz informed PhoneDog that he wanted to keep his Twitter blog, with all of his followers; in return, Kravitz agreed that he would still "tweet" occasionally on behalf of his former company, under a new (Twitter) "handle," or account name, NoahKravitz. Initially, PhoneDog seemed to have no problem with this arrangement. In July 2011, however, PhoneDog sued Kravitz, arguing that his list of Twitter followers was, in fact, a company list. PhoneDog also argued that it had invested a substantial amount of money in growing its customer list, which it considered to be the property of PhoneDog Media. The company has sought $340,000 in damages—the amount that PhoneDog estimated it had lost based on 17,000 customers at $2.50 per customer over an eight-month period (following Kravitz's departure from the company).[18]

2. Identify and evaluate the ethical issues that arise in the following scenario from the three main perspectives of cyberethics that we examined in Chapter 1.3. Explain.

In April 2014, Donald Sterling, then owner of the National Basketball Association (NBA)'s San Diego Clippers, was accused of making racist remarks about African Americans. It turns out that Sterling's then (girl)friend, V. Stiviano, had recorded those remarks on an electronic device and then later decided to make them available to a wider audience. This incident received extensive media coverage in the United States and beyond. Many people were appalled by Sterling's remarks, and some also pointed out the irony in this incident, given that the majority of the players on his basketball team (who were largely responsible for generating income for Sterling) were African Americans. Shortly following the fallout from this controversy, Sterling was forced by the NBA to sell his team to a new owner. While most people agreed that Sterling should resign and be required to relinquish his NBA franchise, some were nevertheless troubled by the manner in which his remarks, which were made in confidence to a close friend, were secretly recorded via a digital device and then (eventually) made available to the public.[19]

The practice of secretly recording someone's private conversations is not exactly new; after all, law enforcement authorities have used "wiring" devices to trap suspected criminals into disclosing information that can lead to their arrests. But the idea that ordinary people, especially those in intimate relationships, can now so easily record conversations in deceptive ways via their tiny digital devices can seem chilling. For example, would this practice influence what intimate friends would be willing (or not willing) to say to each other in (supposed) confidence? Would it also alter our privacy expectations in the future with respect to conversations with romantic partners?

▶ ENDNOTES

1. See, for example, Dan Kedmey, "Hackers Leak Explicit Photos of More than 100 Celebrities," *Time Magazine*, September 1, 2014. Available at http://time.com/3246562/hackers-jennifer-lawrence-cloud-data/. Accessed 9/5/14.
2. Some have used a combination of these two expressions. For example, Ess (2014) uses "information and computer ethics" (ICE) to refer to ethical issues affecting "digital media." And Capurro (2007) uses the expression "Intercultural Information Ethics" (IIE).
3. We should note that others have used the expression ICT (information and communications technology) ethics to describe the field that we refer to as cyberethics, whereas Ess (2014) has recently proposed the expression "digital media ethics." But as in the case of the other competing expressions we have critiqued, these two also fail to capture the breadth of the wide range of topics we cover under the expression "cyberethics."
4. Floridi (2007, p. 63) contrasts Information Ethics (IE) with computer ethics (CE), by noting that the former is the "philosophical foundational counterpart of CE."
5. It is worth noting that some authors have used the term "cyberethics" in ways that are different from the definition proposed here. See, for example, Baird, Ramsower, and Rosenbaum (2000).
6. Anderson and Anderson (2011) also use the term "machine ethics" to refer to this new field, which they describe as one "concerned with giving machines ethical principles." They contrast the development of ethics for people who use machines with the development of ethics for machines. Others, however, such as Lin, Abney, and Bekey (2012), use the expression "robot ethics" to describe this emerging field.
7. See the interview conducted with Paul Ceruzzi in the BBC/PBS video series, *The Machine That Changed the World* (1990).

8. For example, Bynum (2008) notes that Norbert Weiner, in his writings on cybernetics in the late 1940s, anticipated some of these concerns.
9. My analysis of the "four phases" in this section draws from and expands upon some concepts and distinctions introduced in Tavani (2001). Note that what I am 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.
10. Maner (2004, p. 41) argues that computers have generated "entirely new ethical issues, unique to computing, that do not surface in other areas."
11. My description and analysis of the "uniqueness debate" in this section draws from and expands upon some concepts and distinctions introduced in Tavani (2001); for a more extended analysis of this debate, see Tavani (2002a).
12. Moor (2004), p. 107.
13. Gotterbarn (1995), p. 21.
14. Moor (2007), p. 31.
15. Brey (2004), pp. 55–6.
16. For more details regarding this distinction, see Brey (2004), pp. 56–7.
17. See Brey, pp. 64–5. For a discussion of how Brey's interdisciplinary model can also be applied to computer ethics instruction, see Tavani (2002b).
18. See J. Biggs, "A Dispute Over Who Owns a Twitter Account Goes to Court." *New York Times*, December 25, 2011. Available at http://www.nytimes.com/2011/12/26/technology/lawsuit-may-determine-who-owns-a-twitter-account.html?_r=3.
19. See, for example, the account of this incident in http://www.huffingtonpost.com/2014/04/26/donald-sterling-racist_n_5218572.html

▶ REFERENCES

Anderson, Michael, and Susan Leigh Anderson, eds. 2011. *Machine Ethics*. New York: Cambridge University press.

Baird, Robert M., Reagan Ramsower, and Stuart E. Rosenbaum, eds. 2000. *Cyberethics: Moral, Social, and Legal Issues in the Computer Age*. Amherst, NY: Prometheus Books.

Barger, Robert N. 2008. *Computer Ethics: A Case-Based Approach*. New York: Cambridge University Press.

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. Reprinted from *Computers and Society* 30, no. 4 (2000): 10–16.

Brey, Philip. 2005. "Freedom and Privacy in Ambient Intelligence," *Ethics and Information Technology* 7, no. 4: 157–66.

Buchanan, Elizabeth A. 2004. "Ethical Considerations for the Information Professions." In R. A. Spinello and H. T. Tavani, eds. In *Readings in CyberEthics*. 2nd ed. Sudbury, MA: Jones and Bartlett Publishers, pp. 613–24.

Buchanan, Elizabeth A. and Kathrine A. Henderson. 2009. *Case Studies in Library and Information Science Ethics*. Jefferson, NC: McFarland.

Bynum, Terrell Ward. 2008. "Milestones in the History of Information and Computer Ethics." In K. E. Himma and H. T. Tavani, eds. *The Handbook of Information and Computer Ethics*. Hoboken, NJ: John Wiley and Sons, pp. 25–48.

Capurro, Rafael. 2007. "Intercultural Information Ethics." In R. Capurro, J. Freübrauer, and T. Hausmanninger, eds. *Localizing the Internet: Ethical Aspects in Intercultural Perspective*. Munich: Fink Verlag, pp. 21–38.

Ess, Charles. 2014. *Digital Media Ethics*. 2nd ed. London, UK: Polity Press.

Floridi, Luciano. 2007. "Information Ethics: On the Philosophical Foundations of Computer Ethics." In J. Weckert, ed. *Computer Ethics*. Aldershot, UK: Ashgate, pp. 63–82. Reprinted from *Ethics and Information Technology* 1, no. 1 (1999): pp. 37–56.

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.

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. Collste, ed. *Ethics in the Age of Information Technology*. Linköping, Sweden: Centre for Applied Ethics, pp. 17–31.

Johnson, Deborah G. 2010. *Computer Ethics*. 4th ed. Upper Saddle River, NJ: Prentice Hall.

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

Lin, Patrick, Keith Abney, and George A. Bekey, eds. 2012. *Robot Ethics: The Ethical and Social Implications of Robotics*. Cambridge, MA: MIT 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. Reprinted from *Science and Engineering Ethics* 2, no. 2 (1996): 137–54.

Moor, James H. 2001. "The Future of Computer Ethics: You Ain't Seen Nothing Yet." *Ethics and Information Technology* 3, no. 2: 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 Publishers, pp. 407–17. Reprinted from *Ethics and Information Technology* 1, no. 1 (1999): 65–69.

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. 121–38.

Moor, James H. 2007. "What Is Computer Ethics?" In J. Weckert, ed. *Computer Ethics*. Aldershot, UK: Ashgate, pp. 31–40. Reprinted from *Metaphilosophy* 16, no. 4 (1985): 266–75.

Tavani, Herman T. 2001. "The State of Computer Ethics as a Philosophical Field of Inquiry." *Ethics and Information Technology* 3, no. 2: 97–108.

Tavani, Herman T. 2002a. "The Uniqueness Debate in Computer Ethics: What Exactly Is at Issue, and Why Does it Matter?" *Ethics and Information Technology*, 4, no. 1: 37–54.

Tavani, Herman T. 2002b. "Applying an Interdisciplinary Approach to Teaching Computer Ethics." *IEEE Technology and Society Magazine* 21, no. 3: 32–38.

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. Reprinted from *Metaphilosophy*, 28, no. 3 (1997): 234–48.

Wallach, Wendell and Colin Allen. 2009. *Moral Machines: Teaching Robots Right from Wrong*. New York: Oxford University Press.

▶ FURTHER READINGS

Brey, Philip, Adam Briggle, and Edward Spence. 2012. *The Good Life in a Technological Age*. New York: Routledge.

Floridi, Luciano, ed. 2010. *The Cambridge Handbook of Information and Computer Ethics*. Cambridge, MA: MIT Press.

Floridi, Luciano. 2013. *The Ethics of Information*. Oxford University Press.

Heikkero, Topi. 2012. *Ethics in Technology: A Philosophical Study*. Lanham, MD: Lexington Books.

Holbrook, J. Britt and Carl Mitcham, eds. *Ethics, Science, Technology, and Engineering: A Global Resource*. 2nd ed. 2015. 4 Vols. Farmington Hills, MI: Macmillan Reference,.

Mittleman, Daniel, ed. 2014. *Annual Editions: Technologies, Social Media, and Society*. 20th ed. New York: McGraw Hill.

Moor, James H. 2008. "Why We Need Better Ethics for Emerging Technologies." In J. van den Hoven and J. Weckert, eds. *Information Technology and Moral Philosophy*. New York: Cambridge University Press, pp. 26–39.

Sandler, Ronald L., ed. 2014. *Ethics and Emerging Technologies*. New York: Palgrave Macmillan/St. Martin's.

van den Hoven, Jeroen. 2008. "Moral Methodology and Information Technology." In K. E. Himma and H. T. Tavani, eds. *The Handbook of Information and Computer Ethics*. Hoboken, NJ: John Wiley and Sons, pp. 49–67.

Wallach, Wendell. 2015. *A Dangerous Master: How to Keep Technology from Slipping Beyond Our Control*. New York: Basic Books.

▶ ONLINE RESOURCES

Association for Computing—Special Interest Group on Computers and Society. http://www.sigcas.org/

Ethical Issues in the Online World (Santa Clara University). http://www.scu.edu/ethics-center/ethicsblog/internet-ethics.cfm

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

ICT Ethics Bibliography. Annotated bibliographies in ICT (information and Communications Technology) Ethics are included in a series of ten installments (published between 1999 and 2013) in the *Journal Ethics and Information Technology* (http://www.springer.com/computer/swe/journal/10676).

International Center for Information Ethics (ICIE). http://icie.zkm.de/

International Society for Ethics and Information Technology. http://inseit.net/

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

Stanford Encyclopedia of Philosophy. http://plato.stanford.edu/ Includes several articles on topics pertaining to issues in computer/information ethics.