istI

Revision notes - IS1103

Ma Hongqiang

March 8, 2017

Contents

1 Introduction to Cyberethics: Concepts, Perspectives

Definition 1.1 (Cyberethics)**.**
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.(Textbook)
Computer ethics is the analysis of the nature and the social impact of computer technology, and the corresponding formulation and justification ofpolicies, for the ethical use of such technology.

Definition 1.2 (Cybertechnology)**.**
Cybertechnology refers to a wide range of computing and communication devices, from stand-alone computers to connected, or networked, computing and communication technologies.

1.1 Four Developmental Phases in Cybertechnology

Phase 1 (1950s and 1960s)
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 like "Can machines think?" 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 (or AI).
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.

Phase 2 (1970s and 1980s)
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.
Ethical issues associated with this phase of computing included concerns about personal privacy, intellectual property, and computer crime.

Phase 3 (1990—Present)
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.
Issues of jurisdiction also arose because there are no clear national or geographical boundaries in cyberspace.
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.

Phase 4 (Present—Near Future)
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.

Phase	Time Period	Techniogical Features	Associated Issues
1	1950s–1960s	Stand-alone Machines (large mainframe computers)	Artifical intelligence(AI), database privacy("Big Brother")
2	1970s-1980s	Minicomputers and the ARPANET; desktop computers interconnected via privately owned networks	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	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 communication technologies with nanotechnology and biotechnology; increasing use of autonomous systems	Issues from Phases 1-3 plus concerns about artificial electronic agents (bots) with decision-making capabilities, and developments in nanocomputing, bioinformatics, and ambient intelligence

1.2 Are Cyberethic Issues Unique Ethical Issues?

There are two schools of thought regarding this question.
Proponents of the position that Cyberethic issues are not unique could point to the fact that crime activities like bullying are hardly new, since these kinds of activities have been carried out in the off-line world for quite some time. So, cybertechnology might be seen simply as the latest in a series of tools or techniques that are now available to aid bullies in carrying out their activities.
Alternatively, some argue that forms of behavior made possible by cybertechnology have indeed raised either new or special ethical problems. Using the example of cyberbullying to support this view, one might point out the relative ease with which bullying activities can now be carried out. Also consider issues having to do with scope and scale: Bullying activities can now occur on a scale or order of magnitude that could not have been realized in the pre-Internet era. More individuals can now engage in bullying behavior because cybertechnology has made it easy, and, as a result, significantly more people can now become the victims of bullies.
Walter Maner (2004) argues that computer use has generated a series of ethical issues that (a) did not exist before the advent of computing, and (b) could not have existed if computer

technology had not been invented.
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.
However, 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.
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 cybertechnologythat is, issues involving privacy, intellectual property, and so forthmight 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 Moors line of reasoning, that an independent field of applied ethics that focuses on ethical aspects of cybertechnology is indeed justified.

1.3 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. The 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.

1.3.1 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 information-technology (IT) professionals.
Some suggests that some nonprofessional ethics issues must also be examined because of the significant impact they have on noninformation professionals, including ordinary computer users.
However, although computer ethics, as a separate field of applied ethics, may eventually go away, 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, Gotterbarns original model of computer ethics might turn out to be the correct one in the long term.

1.3.2 Cyberethics as a Field of Philosophical Ethics

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 behaviorthat 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. Cyberethics as a branch of philosoplical 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.
Methodology and Philosophical Ethics include three distinct stages:

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.

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

The two perspectives on cyberethics that we have examined thus farprofessional ethics and philosophical ethicscan both be understood as normative inquiries(what *is* the case) 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(what *ought to be* the case) 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.
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. 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.

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

1.4 A Comprehensive Cyberethics Methodology

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 Breys disclosive method is to reveal moral values embedded in the various features and practices associated with cybertechnology itself.
Breys 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 systemdesign 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.19 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. Jeroen 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.

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

1.5 A Comprehensive Strategy for Approaching Cyberethic Issues

The following methodological scheme, which expands on the original three-step scheme introduced, is intended as a strategy to assist you in identifying and analyzing the specific cyberethics issues examined in this book.

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, i.e., social policies or ethical codes, that can help resolve the issue.
- 1d If the normative ethical issue cannot be resolved through the application of existing policies, codes of conduct, etc., 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 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.

2 Ethical Concepts and Ethical Theories: Establishing and Justifying a Moral System

2.1 Ethics and Morality

Definition 2.1 (Ethics)**.** Ethics is the study of morality.

Definition 2.2 (Morality)**.** Morality can be defined as a system of rules for guiding human conduct, and principles for evaluating those rules.

Note that (i) morality is a system, and (ii) it is a system comprised of moral rules and principles. Moral rules can be understood as rules of conduct, which are very similar to the notion of policies. There, policies were defined as rules of conduct that have a wide range of application. According to James Moor (2004), policies range from formal laws to informal, implicit guidelines for actions.
There are two kinds of rules of conduct:

1. *Directives* that guide our conduct as individuals (at the microlevel)

2. *Social policies* framed at the macrolevel

Directives are rules that guide our individual actions and direct us in our moral choices at the microethical level; rules of conduct that operate at the macroethical level guide us in both framing and adhering to social policies. Both types of rules of conduct are derived from a set of core values in a moral system.
The rules of conduct in a moral system are evaluated against standards called principles.

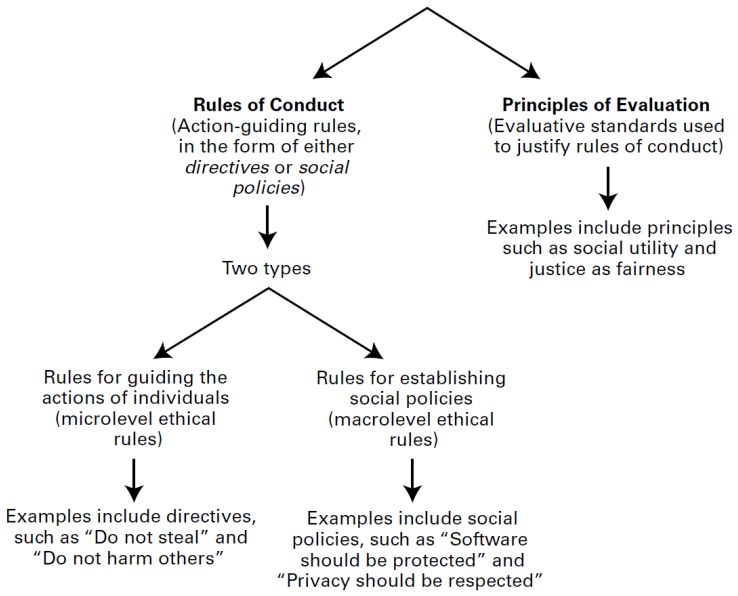
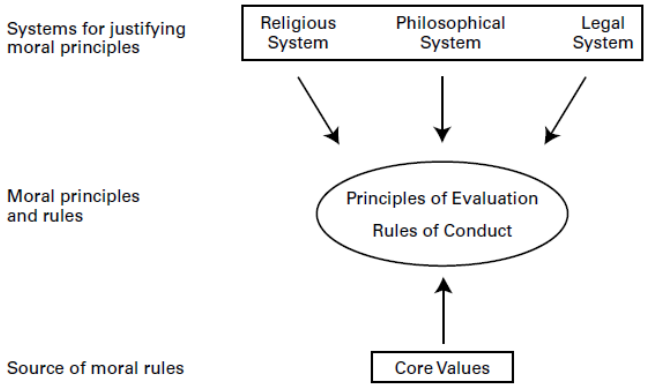


Figure 1: Basic components of a moral system



According to Bernard Gert (2005, 2007), morality is a system whose purpose is to prevent harm and evils. In addition to preventing harm, a moral system aims at promoting human flourishing.

Gert describes a moral system as one that is both public and informal. The system is public, he argues, because everyone must know what the rules are that define it.

Morality is also informal because, Gert notes, a moral system has no formal authoritative judges presiding over it.

Gerts model of a moral system includes two additional features: rationality and impartiality. A moral system is rational in that it is based on principles of logical reason accessible to ordinary persons. Morality cannot involve special knowledge that can be understood only by privileged individuals or groups. The rules in a moral system must be available to all rational persons who, in turn, are (what ethicists call) moral agents, bound by the system of moral rules. We do not hold nonmoral agents (such as young children, mentally challenged persons, and pets) morally responsible for their own actions, but moral agents often have responsibilities to nonmoral agents.

A moral system is impartial in the sense that the moral rules are ideally designed to apply equitably to all participants in the system. In an ideal moral system, all rational persons are willing to accept the rules of the system, even if they do not know in advance what their particular place in that system will be. To ensure that impartiality will be built into a moral system, and that its members will be treated as fairly as possible, Gert invokes his blindfold of justice principle.

On the one hand, rules of conduct for guiding action in the moral system, whether individual

Public	Informal	Rational	Impartial
The rules are known to all of the members.	The rules are informal, not like formal laws in a legal system.	The system is based on principles of logical reason accessible to all its members.	The system is not partial to any one group or individual.

directives or social policies, are ultimately derived from certain core values. Principles for evaluating rules of conduct, on the other hand, are typically grounded in one of three systems or sources: religion, law, or (philosophical) ethics. There are three approaches for grounding the principles in a moral system:

Approach 1: Grounding Moral Principles in a Religious System
Stealing is wrong because it offends God or because it violates one of Gods Ten Commandments.
One difficulty in applying this rationale in the United States is that society is pluralistic.

Approach 2: Grounding Moral Principles in a Legal System
Stealing is wrong because it violates the law.
But laws are not uniform across political boundaries. A more serious flaw in using a legal approach is that history has shown that certain laws, although widely accepted, institutionalized, and practiced within a society, have nonetheless been morally wrong.

Approach 3: Grounding Moral Principles in a Philosophical System of Ethics
Stealing is wrong because it is wrong.

2.2 Discussion Stoppers as Roadblocks to Moral Discourse

2.2.1 Stopper 1: People Disagree on Solutions to Moral Issues

Because different people often have different beliefs as to the correct answer to many moral questions, some infer that there is no hope of reaching any kind of agreement on answers to any moral question. And from this inference, some conclude that any meaningful discourse about morality is impossible. Three crucial points that people who draw these and similar inferences about morality fail to recognize, however, are as follows:

1. Experts in other fields of study, such as science and mathematics, also disagree as to the correct answers to certain questions.

2. There is common agreement as to answers to some moral questions.

3. People do not always distinguish between disagreements about general principles and disagreements about factual matters in disputes involving morality.

2.2.2 Stopper 2: Who Am I to Judge Others?

People are often uncomfortable with the prospect of having to evaluate the moral beliefs and practices of others. We generally feel that it is appropriate to describe the different moral beliefs that others have but that it is inappropriate to make judgments about the moral beliefs held by others. This assumption is problematic at two levels: First, as a matter of descriptive fact, we constantly judge others in the sense that we make certain evaluations about them. And second, from a normative perspective, in certain cases we should make judgments (evaluations) about the beliefs and actions of others.

2.2.3 Stopper 3: Morality Is Simply a Private Matter

Many people assume that morality is essentially personal in nature and must, therefore, be simply a private matter. Initially, such a view might seem reasonable, but it is actually both confused and problematic. In fact, private morality is essentially an oxymoron, or

contradictory notion. For one thing, morality is a public phenomenonrecall our discussion of Gerts account of morality as a public system, where we saw that a moral system includes a set of public rules that apply to all of the members of that system. Thus morality cannot be reduced to something that is simply private or personal.

2.2.4 Stopper 4: Morality Is Simply a Matter for Individual Cultures to Decide

Stopper #1	Stopper #2	Stopper #3	Stopper #4
People disagree on solutions to moral issues.	*Who am I to judge others?*	*Ethics is simply a private matter.*	*Morality is simply a matter for individual cultures to decide.*
1. Fails to recognize that experts in many areas disagree on key issues in their fields.	1. Fails to distinguish between the act of judging and being a judgmental person.	1. Fails to recognize that morality is essentially a public system.	1. Fails to distinguish between descriptive and normative claims about morality.
2. Fails to recognize that there are many moral issues on which people agree.	2. Fails to distinguish between judging as condemning and judging as evaluating.	2. Fails to note that personally based morality can cause major harm to others.	2. Assumes that people can never reach common agreement on some moral principles.
3. Fails to distinguish between disagreements about principles and disagreements about facts.	3. Fails to recognize that sometimes we are required to make judgments.	3. Confuses moral choices with individual or personal preferences.	3. Assumes that a system is moral because a majority in a culture decides it is moral.

2.3 Why do We Need Ethical Theories?

An essential feature of theories in general is that they guide us in our investigations and analyses.Ethical theory, like scientific theory, provides us with a framework for analyzing moral issues via a scheme that is internally coherent and consistent as well as comprehensive and systematic. To be coherent, a theorys individual elements must fit together to form a unified whole. To be consistent, a theorys component parts cannot contradict each other. To be comprehensive, a theory must be able to be applied broadly to a wide range of actions. And to be systematic, a theory cannot simply address individual symptoms peculiar to specific cases while ignoring general principles that would apply in similar cases.

2.4 Consequence-based Ethical Theories

Some have argued that the primary goal of a moral system is to produce desirable consequences or outcomes for its members. For these ethicists, the consequences (i.e., the ends achieved) of actions and policies provide the ultimate standard against which moral decisions must be evaluated. So if one must choose between two courses of action that is, either Act A or Act Bthe morally correct action will be the one that produces the most desirable outcome.

Utilitarians argue that the outcome or consequences for the greatest number of individuals, or the majority, in a given society is paramount in moral deliberation. According to the utilitarian theory,

> An individual act (X) or a social policy (Y) is morally permissible if the consequences that result from (X) or (Y) produce the greatest amount of good for the greatest number of persons affected by the act or policy.

Utilitarians stress the social utility or social usefulness of particular actions and policies by focusing on the consequences that result from those actions and policies. Jeremy Bentham (17481832), who was among the first philosophers to formulate utilitarian ethical theory in a systematic manner, defended this theory via two claims:

1. Social utility is superior to alternative criteria for evaluating moral systems.

2. Social utility can be measured by the amount of happiness produced.

According to (I), the moral value of actions and policies ought to be measured in terms of their social usefulness (rather than via abstract criteria such as individual rights or social justice). The more utility that specific actions and policies have, the more they can be defended as morally permissible actions and policies.

Bentham believed that it is not the maximization of individual pleasure or happiness that is important, but rather generating the greatest amount of happiness for society in general. Since it is assumed that all humans, as individuals, desire happiness, it would follow on utilitarian grounds that those actions and policies that generate the most happiness for the most people are most desirable. Of course, this reasoning assumes:

1. All people desire happiness.

2. Happiness is an intrinsic good that is desired for its own sake.

John Stuart Mill (18061873) offered the following argument for (a):

> The only possible proof showing that something is audible is that people actually hear it; the only possible proof that something is visible is that people actually see it; and the only possible proof that something is desirable is that people actually desire it.

From the fact that people desire happiness, Mill inferred that promoting happiness ought to be the criterion for justifying a moral system. Unlike other goods that humans desire as means to one or more ends, Mill argued that people desire happiness for its own sake. Thus, he concluded that happiness is an intrinsic good.

2.4.1 Act Utilitarianism

According to act utilitarians, An act, X, is morally permissible if the consequences produced by doing X result in the greatest good for the greatest number of persons affected by Act X.
All things being equal, actions that produce the greatest good (happiness) for the greatest number of people seem desirable. However, policies and practices based solely on this principle can also have significant negative implications for those who are not in the majority (i.e., the greatest number).
Critics who reject the emphasis on the consequences of individual acts point out that in our day-to-day activities we tend not to deliberate on each individual action as if that action were unique. Rather, we are inclined to deliberate on the basis of certain principles or general rules that guide our behavior.

2.4.2 Rule Utilitarianism

Some utilitarians argue that the consequences that result from following rules or principles, not the consequences of individual acts, ultimately matter in determining whether or not a certain practice is morally permissible. This version of utilitarian theory, called rule utilitarianism, can be formulated in the following way:
An act, X, is morally permissible if the consequences of following the general rule, Y, of which act X is an instance, would bring about the greatest good for the greatest number.
Policies that can intentionally cause the death of an innocent individual ought not to be allowed, even if the net result of following such policies meant that more human lives would be saved. For one thing, such a policy would seem unfair to all who are adversely affected. But perhaps more importantly from a rule utilitarians perspective, adopting such a policy would not result in the greatest good for society.
Rule utilitarianism would seem to be a more plausible ethical theory than act utilitarianism. However, some critics reject all versions of utilitarianism because they believe that no matter how this theory is expressed, utilitarianism is fundamentally flawed. These critics tend to attack one or both of the following aspects of utilitarian theory:

1. Morality is basically tied to the production of happiness or pleasure.

2. Morality can ultimately be decided by consequences (of either acts or policies).

Critics of utilitarianism argue that morality can be grounded neither in consequences nor in happiness. Hence, they argue that some alternative criterion or standard is needed.

2.5 Duty-based Ethical Theories

Immanuel Kant (17241804) argued that morality must ultimately be grounded in the concept of duty, or obligations that humans have to one another, and never in the consequences of human actions. As such, morality has nothing to do with the promotion of happiness or the achievement of desirable consequences. Thus Kant rejects utilitarianism in particular, and all consequentialist ethical theories in general.Hepoints out that, in some instances, performing our duties may result in our being unhappy and may not necessarily lead to consequences

that are considered desirable. How can a deontological theory avoid the problems that plague consequentialist theories such as utilitarianism? Kant provides two answers to this question, one based on our nature as rational creatures, and the other based on the notion that human beings are ends-inthemselves.

Kant argues that what separates us from other kinds of creatures, and what binds us morally, is our rational capacity. Unlike animals who may be motivated only by sensory pleasure, humans have the ability to reason and deliberate. So Kant reasons that if our primary nature were such that we merely seek happiness or pleasure, as utilitarians suggest, then we would not be distinguishable from other creatures in morally relevant ways. But because we have a rational capacity, we are able to reflect upon situations and make moral choices in a way that other kinds of (nonrational) creatures cannot. Kant argues that our rational nature reveals to us that we have certain duties or obligations to each other as rational beings in a moral community.

We can next examine Kants second argument, which concerns the roles of human beings as ends-in-themselves. We have seen that in focusing on criteria involving the happiness of the majority, utilitarians allow, even if unintentionally, that the interests and well-being of some humans can be sacrificed for the ends of the greatest number. Kant argues that a genuinely moral system would never permit some humans to be treated simply as means to the ends of others. He also believes that if we are willing to use a standard based on consequences (such as social utility) to ground our moral system, then that system will ultimately fail to be a moral system. Kant argues that each individual, regardless of his or her wealth, intelligence, privilege, or circumstance, has the same moral worth. From this, Kant infers that each individual is an end in him- or herself and, therefore, should never be treated merely as a means to some end. Thus we have a duty to treat fellow humans as ends.

2.5.1 Rule Deontology

For Kant, there is such a standard or objective test, which can be formulated in a principle that he calls the categorical imperative, that can be used in an objective and impartial way to determine the basis for our moral obligations.

One variation of his imperative directs us to

Act always on that maxim or principle (or rule) that ensures that all individuals will be treated as ends-in-themselves and never merely as a means to an end.

Another variation of the categorical imperative can be expressed in the following way:

Act always on that maxim or principle (or rule) that can be universally binding, without exception, for all human beings.9

Kant believed that if everyone followed the categorical imperative, we would have a genuinely moral system. It would be a system based on two essential principles: universality and impartiality. In such a system, every individual would be treated fairly since the same rules would apply universally to all persons. And because Kants imperative observes the principle of impartiality, it does not allow for one individual or group to be privileged or favored over another. In other words, if it is morally wrong for you to engage in a certain action, then it is also morally wrong for all persons like youthat is, all rational creatures (or moral agents)to engage in that action. And if you are obligated to perform a certain action, then every moral agent is likewise obligated to perform that action.

In Kants deontological scheme, we do not consider the potential consequences of a certain action or of a certain rule to determine whether that act is morally permissible. Rather, the objective rule to be followedthat is, the litmus test for determining when an action will have moral worthis whether the act complies with the categorical imperative. Take the example of practice of slavery; it is immoral because

1. it allows some humans to be used only as a means to an end; and

2. a practice such as slavery could not be consistently applied in an objective, impartial, and universally binding way.

2.5.2 Act Deontology

Ross argues that when two or more moral duties clash, we have to look at individual situations in order to determine which duty will override another. Like act utilitarians, then, Ross stresses the importance of analyzing individual situations to determine the morally appropriate course of action to take. Unlike utilitarians, however, Ross believes that we must not consider the consequences of those actions in deliberating over which course of action morally trumps, or outweighs, another. Like Kant, Ross believes that the notion of duty is the ultimate criterion for determining morality. But unlike Kant, Ross does not believe that blind adherence to certain maxims or rules can work in every case for determining which duties we must ultimately carry out.
Ross believes that we have certain *prima facie* (or self-evident) duties, which, all things being equal, we must follow. He provides a list of *prima facie* duties such as honesty, benevolence, justice, and so forth. For example, each of us has a *prima facie* duty not to lie and a *prima facie* duty to keep a promise. And if there are no conflicts in a given situation, then each *prima facie* duty is also what he calls an actual duty. But how are we to determine what our actual duty is in situations where two or more *prima facie* duties conflict with one another? Ross believes that our ability to determine what our actual duty will be in a particular situation is made possible through a process of rational intuitionism. We saw that for Kant, every *prima facie* duty is, in effect, an absolute duty because it applies to every human being without exception. We also saw that Kants scheme does not provide a procedure for deciding what we should do when two or more duties conflict. However, Ross believes that we can determine what our overriding duty is in such situations by using a deliberative process that requires two steps:

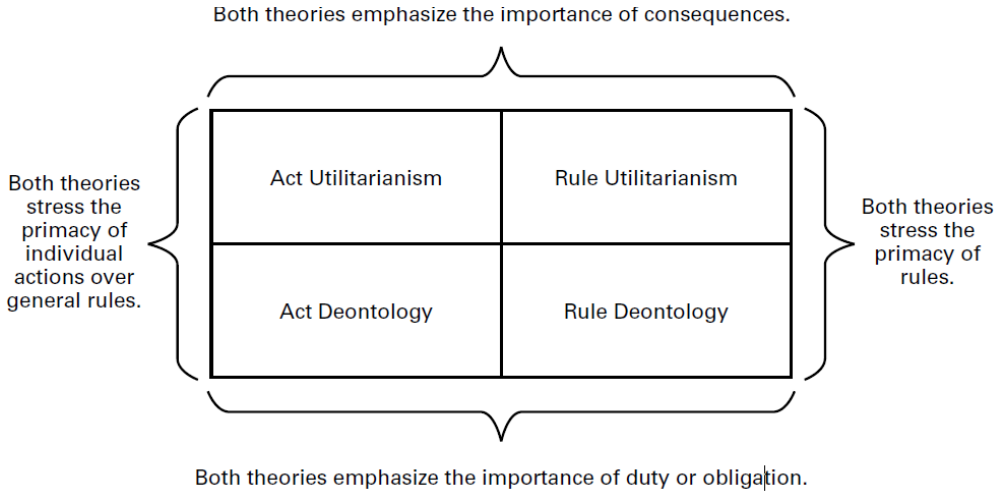
1. Reflect on the competing *prima facie* duties.

2. Weigh the evidence at hand to determine which course of action would be required in a particular circumstance.

Notice that in cases of weighing between conflicting duties, Ross places the emphasis of deliberation on certain aspects of the particular situation or context, rather than on mere deliberation about the general rules themselves. Unlike utilitarians, however, Ross does not appeal to the consequences of either actions or rules in determining whether a particular course of action is morally acceptable. For one thing, Ross argues that he would have to be omniscient to know what consequences would result from his actions. So, like all

deontologists, Ross rejects the criteria of consequences as a viable one for resolving ethical dilemmas.

One difficulty for Rosss position is that, as noted above, it uses a process called rational intuitionism. Appealing to the intuitive process used in mathematics to justify certain basic mathematical concepts and axioms, Ross believes that the same process can be used in morality. However, his position on moral intuitionism is controversial and has not been widely accepted by contemporary ethicists. And since intuitionism is an important component in Rosss theory of act deontology, many ethicists who otherwise might be inclined to adopt Rosss theory have been skeptical of it. Nevertheless, variations of that theory have been adopted by contemporary deontologists.



2.6 Contract-based Ethical Theories

From the perspective of some social contract theories, a moral system comes into being by virtue of certain contractual agreements between individuals. According to Hobbes, our natural (or physical) constitution is such that in the state of nature we act in ways that will enable us to satisfy our desires (or appetites) and to avoid what Hobbes calls our aversions. While there is a sense of freedomin this natural state, the condition of our day-to-day existence is hardly ideal. In this state, each person must continually fend for herself, and, as a result, each must also avoid the constant threats of others, who are inclined to pursue their own interests and desires.

Hobbes describes this state of nature as one in which life is solitary, poor, nasty, brutish, and short. Because we are rational creatures, and because we see that it would be in our best interests to band together, Hobbes notes that we eventually establish a formal legal code. In doing this, Hobbes believes that we are willing to surrender some of our absolute freedoms to a sovereign. In return, we receive many benefits, including a system of rules and laws that are designed and enforced to protect individuals from being harmed by other members of the system.

One virtue of the social contract model of ethics is that it gives us a motivation for being moral.We see that it is in our individual self-interest to develop a moral systemwith rules.

This type of motivation for establishing a moral system is conspicuously absent in both the utilitarian and deontological theories. So a contract-based ethical theory might seem to have one advantage over them.

2.6.1 Some Criticisms of Contract-based Theories

Some critics, such as Pojman (2006), point out that contract-based theories provide the foundation for only a minimalist morality. They are minimalist in the sense that we are obligated to behave morally only where an explicit or formal contract exists. Of course, we can think of many situations involving morality where there are no express contracts or explicit laws describing our obligations to each other. Yet we also tend to believe that in at least some of these cases we are morally obligated to help others when it is in our power to do so.

Another way to think about minimalist morality is to think of the difference between two principles: (a) doing no harm, and (b) doing good.Aminimalist morality would insist merely that we do not harm others. As such, it does not require that we come to the aid of others.

2.7 Character-based Ethical Theories

A fourth type of ethical theory that must be considered, especially in light of the recent attention it has received, is virtue ethics (also sometimes described as character ethics). This ethical theory ignores the special roles that consequences, duties, and social contracts play in moral systems, especially with respect to determining the appropriate standard for evaluating moral behavior. Rather, it focuses on criteria having to do with the character development of individuals and their acquisition of good character traits from the kinds of habits they develop.

2.7.1 Being a Moral Person vs. Following Moral Rules

Aristotle believed that ethics was something not merely to be studied, but rather to be lived or practiced. In fact, Aristotle thought of ethics as a practical science, like politics. To become an ethical person, in Aristotles view, one is required to do more than simply memorize and deliberate on certain kinds of rules. What is also needed, Aristotle argued, is that people develop certain virtues. Aristotle believed that to be a moral person, one had to acquire the right virtues (strengths or excellences). Through the proper training and acquisition of good habits and character traits, Aristotle believed that one could achieve moral virtues such as temperance and courage that are needed to live well.

Because virtue ethics focuses primarily on character development and moral education, it does not need to rely on a system of formal rules. Virtue ethicists take a very different tack. Instead of asking, What should I do in such and such a situation? a virtue ethicist asks, What kind of person should I be? Hence, the emphasis on being a moral person, and not simply on understanding what moral rules are and how they apply in certain situations. Whereas deontological and utilitarian theories are action-oriented and rule-oriented, virtue ethics is agent-oriented because it is centered on the moral development and character of the agent herself.

Virtue ethicists believe that a moral person is one who is necessarily disposed to do the right thing. They correctly point out that when we engage in routine acts in our daily lives, including many of our nonnormative actions, we do not deliberate by asking ourselves, What ought I to do in such and such a case? A virtue ethicist would point out that if that person had developed the right kind of moral character (through the acquisition of the correct moral habits), he or she would not be in a position that required such deliberation.
It would seem that the re-emergence of virtue ethics, despite the fact that its origins can be traced back to classical Greece, has provided ethicists with some fresh insights. However, we should also note that virtue ethics is not without its critics. One of the chief drawbacks of taking virtue ethics as a complete theory of ethics is that it neither helps resolve conflicts that can arise among the competing virtues nor encourages examination of consequences. Some critics point out that a virtue- or character-based ethics would seem to have a better chance of taking hold in a society that is homogeneous rather than in one that is heterogeneous or pluralistic.
It is also worth pointing out that character-based ethical systems would most likely flourish in cultures where the emphasis placed on community life is stronger than that accorded to the role of individuals themselves.

2.8 Integrating aspects of Classical Ethical Theories into a Single Comprehensive Theory

Type of Theory	Advantages	Disadvantages
Consequence-based (utilitarian)	Stresses promotion of happiness and utility	Ignores concerns of justice for the minority population
Duty-based (deontology)	Stresses the role of duty and respect for persons	Underestimates the importance of happiness and social utility
Contract-based (rights)	Provides a motivation for morality	Offers only a minimal morality
Character-based (virtue)	Stresses character development and moral education	Depends on homogeneous community standards for morality

Figure 2: Four types of ethical theories

Influenced by the work of Gert and others, Moor (2004) has proposed a scheme that integrates aspects of utilitarian and deontological theories into a framework he calls just consequentialism.

2.8.1 Moor's Just-Consequentialist Theory and its Application to Cybertechnology

Moor believes that only an ethical approach that combines considerations of consequences of action with more traditional deontological considerations of duties, rights, and justice can provide us with a defensible ethical theoryviz., just consequentialismthat yields a useful framework for applied ethics. Moor begins by considering what kind of conduct we want

ethics to regulate. He believes first and foremost everyone wants to be protected against suffering unnecessary harms. We dont want to be killed or suffer great pain or have our freedom taken away. Human nature is such that people value the same kind of basic goods (life, happiness, abilities, security, knowledge, freedom, opportunities, and resources). The specifics of these may manifest somewhat differently in different cultures (some kinds of freedom may be more important in some cultures than others, for example), but the general set of goods, which Moor calls core values (see Section 2.1.2), is shared by all. Losing any of these goods counts as harm, and all of us want ethics to protect us from others causing us harm. This point is captured by the familiar ethical maxim Do no harm, described earlier.

Another desirable objective of ethics, according toMoor, is to support justice, rights, and duties. We want others to keep their promises and agreements, to obey the law, and to fulfill their duties in whatever roles they play. These specific obligations are generated within societies, and to the extent that they spring from just agreements, laws, and social situations, we justifiably expect others to fulfill their duties toward us. Another familiar maxim of ethics is Do your duty, where duty here designates specific duties people acquire by their roles in society such as a signer of contract, a citizen, a parent, an employer, or an employee.

Moor believes that if all we had to do to be ethical were to do no harm and perform our duties, ethics would be challenging but at least easy to understand. But, as Moor argues, the ethical life is not nearly so simple. Often actions involve a mixture of goods and evils as well as conflicts among duties. Sometimes we need to make exceptions to our general policies for action. How do we decide what to do? His answer involves two steps: the *deliberation* stage and the selection stage. First, at the deliberation stage, we should consider the various possible policies for action from an impartial point of view. Impartial does not mean that everyone is treated the same but that the policy is regarded as a rule governing the situation without consideration of the particular individuals who happen to be involved. This is what Gert has in mind by his blindfold of justice (see Section 2.1.1) or what Rawls suggests with his veil of ignorance. This is a technique to establish the justice of a policyit will not be just if one will not accept the policy as a general rule of conduct, not knowing who plays which roles in the situation.

However, many policies will pass the impartiality test, and we will still need to consider whether we should adopt them. We need to move to the second step in the decision-making process, the *selection* stage, and carefully weigh the good consequences and the bad consequences of the remaining policies. In this second step, it may be less of a choice between ethical vs. unethical policies than between better vs. worse policies. Although we may be able to at least partially rank policies, legitimate disagreements about the rankings often exist.

According to Moor, it is important to keep in mind that although we may disagree about the merits of various policies and how to rank them, rational discussion of the relevant policies is very possible and highly desirable. People may overlook values embedded in a situation and may change their rankings once informed. People may not be fully aware of the consequences of various policies. Moor does not believe that complete agreement on controversial policies can or necessarily should be reached, as people may ultimately rank benefits and harms differently. Nevertheless, considerable consensus about some policies

being better than others can often be generated. Moor points out that frequently much of the disagreement hinges on differences about the facts of the case than on value differences.

2.9 Key Elements in Moor's Just-Consequentialist Framework

Moors ethical framework of just consequentialism can be summarized in terms of a strategy that includes the following steps:

1. Deliberate over various policies from an impartial point of view to determine whether they meet the criteria for being ethical policies. A policy is ethical, if it
   (a) does not cause any unnecessary harms to individuals and groups, and
   (b) supports individual rights, the fulfilling of duties, etc.
2. Select the best policy from the set of just policies arrived at in the deliberation stage by ranking ethical policies in terms of benefits and (justifiable) harms. In doing this, be sure to
   (a) weigh carefully between the good consequences and bad consequences in the ethical policies, and
   (b) distinguish between disagreements about facts and disagreements about principles and values, when deciding which particular ethical policy should be adopted. (Knowledge about the facts surrounding a particular case should inform the decision-making process.)

As we noted in our discussion of virtue ethics in Section 2.7.2, Moor points out that developing the appropriate habits of character such as kindness, truthfulness, honesty, trustworthiness, helpfulness, generosity, and justice is an important prerequisite in moral behavior. So if one has not already developed the correct habits required for moral behavior, it may be difficult for an individual to successfully carry out the steps in Moors just-consequentialist model. In this sense, elements of virtue ethics or character-based ethics are also presupposed in Moors framework.

3 Privacy and Cyberspace

3.1 Are Privacy Concerns Associated With Cybertechnology Unique or Special?

Concerns about personal privacy existed long before the advent of computers and cybertechnology. What, if anything, is special about the privacy concerns that are associated with cybertechnology? Then consider the impact that changes involving this technology have had on privacy with respect to the

- *amount* of personal information that can be collect,
- *speed* at which personal information can be transmitted,
- *duration* of time that the information can be retained,
- *kind* of information that can be acquired and exchanged.

Additionally, we should note that cybertechnology raises privacy concerns because of the myriad ways in which it enables our personal information to be *manipulated* (e.g., merged, matched, and mined) once it has been collected.

3.2 What is Personal Privacy?

There is no universally agreed upon definition of this concept.
Sometimes we speak of privacy as something that can be lost or diminished, suggesting that privacy can be understood in terms of a repository of personal information that can be either diminished altogether or gradually eroded.
Contrast this view with descriptions of privacy as something that can be intruded upon or invaded, where privacy can be understood in terms of a spatial metaphor, such as a zone, that deserves protection.
Alternatively, privacy is sometimes described as something that can be violated or breached, when we think of it in terms of either a right or an interest that deserves legal protection.
Privacy analysts have pointed out that in the United States, the meaning of privacy has evolved since the eighteenth century. Initially, privacy was understood in terms of freedom from (physical) intrusion. Later it became associated with freedom from interference into ones personal affairs, including ones ability to make decisions freely. Most recently, privacy has come to be closely identified with concerns affecting access to and control of personal informationa view that is also referred to as informational privacy.

3.2.1 Accessibility Privacy: Freedom from Unwarranted Intrusion

In a seminal paper on privacy, SamuelWarren and Louis Brandeis suggested that privacy could be understood as being let alone or being free from intrusion.

3.2.2 Decisional Privacy: Freedom from Interference in One's Personal Affairs

Privacy is also sometimes conceived of as freedom from interference in ones personal choices, plans, and decisions; some refer to this view as decisional privacy.

3.2.3 Informational Privacy: Control over the Flow of Personal Information

Because of the increasing use of technology to gather and exchange personal information, many contemporary analysts view privacy in connection with ones ability to restrict access to and control the flow of ones personal information

3.2.4 A Comprehensive Account of Privacy

James Moor (2000) has introduced an account of privacy that incorporates important elements of the nonintrusion, noninterference, and informational views of privacy. According to Moor,

> An individual [has] privacy in a situation with regard to others if and only if in that situation the individual [is] protected from intrusion, interference, and information access by others.

An important element in this definition is Moors notion of situation, which he deliberately leaves broad so that it can apply to a range of contexts, or zones, that can be declared private.

Central to Moors theory is a distinction between *naturally private* and *normatively private* situations, enabling us to differentiate between the conditions required for (a) having privacy and (b) having a right to privacy. This distinction, in turn, enables us to differentiate between a loss of privacy and a violation of privacy.

In a naturally private situation, individuals are protected from access and interference from others by natural means, for example, physical boundaries such as those one enjoys while hiking alone in the woods. In this case, privacy can be lost but not violated, because there are no normsconventional, legal, or ethicalaccording to which one has a right, or even an expectation, to be protected.

In a normatively private situation, on the other hand, individuals are protected by conventional norms (e.g., formal laws and informal policies) because they involve certain kinds of zones or contexts that we have determined to need normative protection.

3.2.5 Privacy as "Contextual Integrity"

We have seen the important role that a situation, or context, plays in Moors privacy theory. But some critics argue that the meaning of a situation or context is either too broad or too vague. Helen Nissenbaum (2004a, 2010) elaborates on the notion of a context in her model of privacy as contextual integrity, where she links adequate privacy protection to norms of specific contexts. She notes that the things we do, including the transactions and events that occur in our daily lives, all take place in some context or other. In her scheme, contexts include spheres of life such as education, politics, the marketplace, and so forth.

Nissenbaums privacy framework requires that the processes used in gathering and disseminating information (a) are appropriate to a particular context and (b) comply with

norms that govern the flow of personal information in a given context. She refers to these two types of informational norms as follows:

1. Norms of appropriateness

2. Norms of distribution

Whereas norms of appropriateness determine whether a given type of personal information is either appropriate or inappropriate to divulge within a particular context, norms of distribution restrict or limit the flow of information within and across contexts. When either norm has been breached, a violation of privacy occurs; conversely, the contextual integrity of the flow of personal information is maintained when both kinds of norms are respected.
As in the case of Moors privacy model, Nissenbaums theory demonstrates why we must always attend to the context in which information flows, and not to the nature of the information itself, in determining whether normative protection is needed.

3.3 Why is Privacy Important?

Alan Westin believes that countries with strong democratic political institutions consider privacy more important than do less democratic ones. Even though privacy has at least some universal appeal, it is not valued to the same degree in all nations and cultures. As a result, it may be difficult to get universal agreement on privacy laws and policies in cyberspace.

3.4 Is Privacy an Intrinsic Value?

While few would argue that privacy is an intrinsic value, desired for its own sake, others, including Charles Fried (1990), argue that privacy is not merely an instrumental value or instrumental good. Fried suggests that unlike most instrumental values that are simply one means among others for achieving a desired end, privacy is also essential, that is, necessary to achieve some important human ends, such as trust and friendship. We tend to associate intrinsic values with necessary conditions and instrumental values with contingent, or nonnecessary conditions; so while privacy is instrumental in that it is a means to certain human ends, Fried argues that it is also a necessary condition for achieving those ends.
Although agreeing with Frieds claim that privacy is more than merely an instrumental value, James Moor (2004) takes a different approach to illustrate this point. Like Fried, Moor argues that privacy itself is not an intrinsic value. Moor believes that privacy is an articulation, or expression of the core value security, which in turn is essential across cultures, for human flourishing. And like Fried, Moor shows why privacy is necessary to achieve certain ends. Moor further suggests that as information technology insinuates itself more and more into our everyday lives, privacy becomes increasingly important for expressing (the core value) security. Does privacy play a key role in promoting human well-being, as Richard Spinello (2010) claims? Perhaps one way it does is by serving as a shield that protects us from interference. Judith DeCew (2006), who believes that the value of privacy lies in the freedom and independence it provides for us, argues that privacy shields us from pressures that preclude self-expression and the development of

relationships. She claims that privacy also acts as a shield by protecting us from coercion and the pressure to conform. In her view, the loss of privacy leaves us vulnerable and threatened because we are likely to become more conformist and less individualistic.

3.4.1 Privacy as a Social Value

some authors have pointed out the social value that privacy also provides, noting that privacy is essential for democracy. Priscilla Regan (1995) points out that we often frame debates over privacy simply in terms of how to balance privacy interests as individual goods against interests involving the larger social good; in such debates, Regan believes, interests benefiting the social good will generally override concerns regarding individual privacy. If, however, privacy is understood as not solely concerned with individual good but as contributing to the broader social good, then in debates involving the balancing of competing values, individual privacy might have a greater chance of receiving equal consideration.
Since privacy can be of value for greater social goods, such as democracy, as well as for individual autonomy and choice, it would seem that it is important and worth protecting. But privacy is increasingly threatened by new cyber and cyber-related technologies.
Privacy is threatened by three different kinds of practices that use cybertechnology:

1. *Data gathering* techniques used to collect and record personal information, often without the knowledge and consent of users.

2. *Data exchange* techniques used to transfer and exchange personal data across and between computer databases, typically without the knowledge and consent of users.

3. *Data mining* techniques used to search large databases in order to generate consumer profiles based on the behavioral patterns of certain groups.

3.5 Gathering Personal Data: Monitoring, Recording, and Tracking Technologies

Cybertechnology makes it possible to collect data about individuals without their knowledge and consent. In this section, we examine some controversial ways in which cybertechnology is used to gather and record personal data, as well as to monitor and track the activities and locations of individuals.

3.5.1 "Dataveillance" Techniques

Some believe that the greatest threat posed to personal privacy by cybertechnology lies in its capacity for surveillance and monitoring. Others worry less about the monitoring per se and more about the vast amounts of transactional data recorded using cybertechnology. Roger Clarke uses the term dataveillance to capture both the surveillance(data monitoring) and data recording techniques made possible by computer technology.
There are, then, two distinct controversies about dataveillance: one having to do with surveillance as a form of data monitoring, and one having to do with the recording and processing of data once the data are collected.

First, we should note the obvious, but relevant, point that privacy threats associated with surveillance are by no means peculiar to cybertechnology. So surveillance is neither a recent concern nor one that should be associated exclusively with the use of cybertechnology to monitor and record an individuals online activities. However, surveillance has clearly been exacerbated by cybertechnology.
Now, we consider surveillance techniques that involve non-workplace related monitoring and recording of personal data in both off- and online activities. Although users may not always realize that they are under surveillance, their online activities are tracked by Web site owners and operators to determine how frequently users visit their sites and to draw conclusions about the preferences users show while accessing their sites.Wenext consider some controversies associated with a type of online surveillance technology known as *cookies*.

3.5.2 Internet Cookies

Cookies are files that Web sites send to and retrieve from the computer systems of Web users, enabling Web site owners to collect information about an individuals online browsing preferences whenever a person visits a Web site. The use of cookies by Web site owners and operators has generated considerable controversy, in large part because of the novel way that information about Web users is collected and stored. Data recorded about the user are stored on a file placed on the hard drive of the users computer system; this information can then be retrieved from the users system and resubmitted to a Web site the next time the user accesses that site.
Those who defend the use of cookies tend to be owners and operators of Web sites. Proprietors of these sites maintain that they are performing a service for repeat users of a Web site by customizing the users means of information retrieval. They also point out that, because of cookies, they are able to provide a user with a list of preferences for future visits to that Web site. Privacy advocates, on the other hand, see the matter quite differently. They argue that activities involving the monitoring and recording of an individuals activities while visiting a Web site and the subsequent downloading of that information onto a users computer (without informing the user) clearly cross the privacy line. Some privacy advocates also point out that information gathered about a user via cookies can eventually be acquired by online advertising agencies, which can then target that user for online ads.
Initially, you might feel a sense of relief in discovering that, generally, owners and operators of one Web site cannot access cookies-related information pertaining to a users activities on anotherWeb site. However, information about a users activities on different Web sites can, under certain circumstances, be compiled and aggregated by online advertising agencies such as DoubleClick that pay to place advertisements on Web sites. DoubleClick can also acquire information about you from data that it retrieves from other Web sites you have visited and where DoubleClick advertises. The information can then be combined and cross-referenced in ways that enable a marketing profile of that users online activities to be constructed and used in more direct advertisements.
Several privacy advocates have argued that because cookies technology involves monitoring and recording a users activities while visiting Web sites (without the users knowledge and

consent) as well as the subsequent downloading of that information onto a users computer system, it violates the users privacy. To assist Internet users in their concerns about cookies, a number of privacy-enhancing tools, which are discussed in detail in Section 5.8, are available. In most Web browsers, users now also have an option to disable cookies, so that they can either opt-in or opt-out of cookies, assuming that they (i) are aware of cookies technology and (ii) know how to enable/disable that technology on their Web browsers. However, some Web sites will not grant users access unless they accept cookies.
Many privacy advocates object to the fact that the default status for most Web browsers is such that cookies will automatically be accepted unless explicitly overridden by the user. As we noted above, cookies technology involves downloading the information it gathers about users onto the users computer system. So, cookies technology also raises concerns involving encroachment or intrusion into a users physical space as well as privacy concerns regarding the clandestine method used to gather data about users who visit Web sites.

3.5.3 RFID Technology

Another mode of surveillance made possible by cybertechnology involves the use of RFID technology. In its simplest form, RFID technology consists of a tag (microchip) and a reader. The tag has an electronic circuit, which stores data, and an antenna that broadcasts data by radio waves in response to a signal from a reader. The reader also contains an antenna that receives the radio signal, and it has a demodulator that transforms the analog radio information into suitable data for any computer processing that will be done (Lockton and Rosenberg 2005).
Although the commercial use of RFIDs was intended mainly for the unique identification of real-world objects (e.g., items sold in supermarkets), the tags can also be used to monitor those objects after they are sold. For example, Helen Nissenbaum notes that prior to the use of RFID tags

> ...customers could assume that sales assistants, store managers, or company leaders recorded point-of-sale information. RFID tags extend the duration of the relationships, making available to ... others a range of information about customers that was not previously available

In one sense, the use of these tags in inventory control would seem uncontroversial. For example, Simson Garfinkel (2002) notes that a company such as Playtex could place an RFID tag in each bra to make sure that shipments of bras headed for Asia are not diverted to New York. He also points out, however, that a man with a handheld (RFID) reader in his pocket who is standing next to a woman wearing such a bra can learn the make and size of her bra. Additionally, and perhaps more controversially, RFID technology can be used for tracking the owners of the items that have these tags. So, on the one hand, RFID transponders in the form of smart labels make it much easier to track inventory and protect goods from theft or imitation. On the other hand, these tags pose a significant threat to individual privacy. Critics of this technology, which include organizations such as the Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU), worry about the accumulation of RFID transaction data by RFID owners and how those data will be used in the future.
RFID technology is already widely usedas Garfinkel notes, it has been incorporated into

everything from automobile keys to inventory control systems to passports.
Alison Adam (2005) fears that we may come to rely too heavily on these technologies. Because RFID technology is now included in chips being embedded in humans, which enables them to be tracked, it has raised concerns for many privacy advocates.
In light of these and related privacy concerns, Garfinkel has proposed an RFID Bill of Rights to protect individuals and guide businesses that use RFID tags. In this scheme, individuals would have the right to (a) know whether products contain RFID tags, (b) have the tags removed or deactivated when they purchase products, (c) access the tags stored data, and (d) know when, where, and why the tags are being read.
Like Internet cookies and other online data gathering and surveillance techniques, RFID clearly threatens individual privacy. But unlike surveillance concerns associated with cookies, which track a users habits while visiting Web sites, RFID technology can be used to track an individuals location in the offline world.Weexamine some specific privacy and surveillance concerns affecting RFIDin connection with location privacy and pervasive surveillance issues in Chapter 12 in our discussion of ambient intelligence.

3.5.4 Cybertechonology and Government Surveillance

Another mode of surveillance that is also associated with cybertechnology involves governments and government agencies that monitor the activities of citizens, a practice that is sometimes referred to as domestic spying. As already noted, this practice is not exactly new, but as the technologies used by governments to monitor their citizens activities become more sophisticated, intrusive, and pervasive, the threats posed to privacy and civil liberties become exacerbated.
Some cybertechnologies, despite their initial objectives and intent, can facilitate government surveillance. Government agencies currently use a variety of technologies that enable them to intercept and read private e-mail messages.
While few would object to the desirable ends that increased security provides, we will see that many oppose the meansi.e., the specific technologies and programs supporting surveillance operations, as well as legislation. Our purpose in this section has been to briefly describe how government surveillance of citizens illustrates one more way that cybertechnology both contributes to and enhances the ability of organizations to gather and record data about individuals.

3.6 Exchanging Personal Data: Merging and Matching Electronic Records

In the previous section, we examined ways in which personal data could be gathered using surveillance techniques and then recorded electronically in computer databases. Other tools have been devised to transfer and exchange those records across and between computer databases. Simply collecting and recording personal data, per se, might not seem terribly controversial if, for example, the data were never used, transferred, exchanged, combined, or recombined. Some would argue, however, that the mere collection of personal data is problematic from a privacy perspective, assuming that if data are being collected,

there must be some motive or purpose for their collection. Of course, the reason, as many now realize, is that transactions involving the sale and exchange of personal data are a growing business.
Much of the personal data gathered electronically by one organization is later exchanged with other organizations; indeed, the very existence of certain institutions depends on the exchange and sale of personal information. These techniques include computer merging and computer matching.

3.6.1 Merging Computerised Records

Few would dispute the claimthat organizations, in both the public and the private sectors, have a legitimate need for information about individuals in order to make intelligent decisions concerning those individuals. However, few would also disagree with the claim that individuals should have a right to keep some personal information private. A crucial question, then, is: What kind of control can an individual expect to retain over the personal information that he or she has given to an organization?
Computer merging is the technique of extracting information from two or more unrelated databases that contain information about some individual or group of individuals, and then integrating that information into a composite file. It occurs whenever two or more disparate pieces of information contained in separate databases are combined.
When organizations merge information about you in a way that you did not specifically authorize, the contextual integrity of your information has been violated.

3.6.2 Matching Computerised Records

Computer matching is a variation of the technology used to merge computerized records. It involves cross-checking information in two or more unrelated databases to produce matching records, or hits. In federal and state government applications, this technique has been used by various agencies and departments for the express purpose of creating a new file containing a list of potential law violators, as well as individuals who have actually broken the law or who are suspected of having broken the law.
In filling out the various governmental forms, you agreed to give some information to each government agency. It is by no means clear, however, that you authorized information given to any one agency to be exchanged with other agencies. You had no say in the way information that you authorized for use in one context was subsequently used in another. Because of this contextual violation of personal information, some have argued that practices involving computerized matching of records containing personal data raise serious threats for personal privacy. The debate over computerized record matching has been hotly contested, and it has been denounced because of its implications for stereotyping and profiling certain classes or groups of individuals. Computerized record matching has also been criticized by civil liberties groups who fear that such a practice might lead to a new form of social control. Defenders of this practice justify the matching of computer records because it enables us to track down deadbeat parents, welfare cheats, and the like. Although few would object to the ends that could be achieved, we can question whether the practice of computerized matching

is compatible with individual privacy. Even if computerized record matching does help to root out governmental waste and fraud, would that fact alone justify such a practice? Critics have pointed out that computer matches have been made even when there was no suspicion that a particular individual or group of individuals had violated the law.
One line of argumentation sometimes used to defend a practice such as computer matching against the charge of violating privacy rights is as follows:

PREMISE 1 Privacy is a legal right.

PREMISE 2 Legal rights are conditional, not absolute.

PREMISE 3 When one violates the law (i.e., commits a crime), one forfeits ones legal rights.

CONCLUSION: Criminals have forfeited their legal right to privacy.
Initially, this line of reasoning seems quite plausible, but does it apply in the case of computerized record matching? First of all, this argument assumes that we have an explicit legal right to privacy. Let us assume, for the sake of argument, that we have such a right and that all legal rights are (or ought to be) conditional only. Even with the addition of these two assumptions, problems remain: for example, those who maintain that a deadbeat parent has, in violating the law, given up his right to privacy seem to either disregard or ignore any right to privacy accorded to individuals who have not broken the law. For it was only by matching the records of mostly innocent individuals whose names were included in multiple government databases that a hit, identifying one or more alleged criminals, was generated. So even if criminals do forfeit their right to privacy, the process of identifying these criminals via computerized record matching entails that several noncriminals will be required to forfeit that right as well.

3.7 Mining Personal Data

A form of data analysis that uses techniques gained from research and development in artificial intelligence (AI), has been used to mine personal data. Formally referred to as Knowledge Discovery in Databases, or KDD, the process is now more commonly known as data mining.
Essentially, data mining involves the indirect gathering of personal information through an analysis of implicit patterns discoverable in data. Data mining activities can generate new and sometimes nonobvious classifications or categories; as a result, individuals whose data are mined can become identified with or linked to certain newly created groups that they might never have imagined to exist. This is further complicated by the fact that current privacy laws offer individuals virtually no protection with respect to how information about them acquired through data mining activities is subsequently used, even though important decisions can be made about those individuals based on the patterns found in the mined personal data. So, data mining technology can be used in ways that raise special concerns for personal privacy.

3.8 How does Data Mining Threaten Personal Privacy?

For one thing, privacy laws as well as informal data protection guidelines have been established for protecting personal data that are

- *explicit* in databases (in the form of specific electronic records),
- confidential in nature (e.g., data involving medical, financial, or academic records),
- exchanged between or across databases.

However, virtually no legal or normative protections apply to personal data manipulated in the data mining process, where personal information is typically

- implicit in the data,
- nonconfidential in nature,
- not exchanged between databases.

Unlike personal data that reside in explicit records in databases, information acquired about persons via data mining is often derived from implicit patterns in the data. The patterns can suggest new facts, relationships, or associations about a person, placing that person in a newly discovered category or group. Also, because most personal data collected and used in data mining applications is considered neither confidential nor intimate in nature, there is a tendency to presume that such data must, by default, be *public* data. And unlike the personal data that are often exchanged between or across two or more databases in traditional database retrieval processes, in the data mining process personal data are often manipulated within a single database, and typically within a large *data warehouse*.
It is in this senseunauthorized internal use by data usersthat data mining raises serious concerns for personal privacy.
We have seen how data mining can be used to threaten consumer privacy. But can it also be used to protect consumers against fraudulent activities? Perhaps not surprisingly, data mining, like other technologies, can be viewed as a double-edged sword with respect to consumers interests.

3.8.1 Web Mining

Initially, the mining of personal data depended on large (offline) commercial databases called data warehouses, which stored the data, consisting primarily of transactional information. Data mining techniques are now also used by commercial Web sites to analyze data about Internet users, which can then be sold to third parties. This process is sometimes referred to as Web mining, which has been defined as the application of data mining techniques to discover patterns from the Web.
Because the amount of data on the Internet is so vast, one might assume that it is impossible to mine those data in ways that could be useful. However, current data mining tools employ sophisticated and advanced AI technology that enable the users of those tools to comb through massive amounts of data that would not have been possible to analyze

with traditional information retrieval techniques. Also, sophisticated search engines have programs (called spiders) that crawl through the Web in order to uncover general patterns in information across multiple Web sites.

Data Merging	A data exchange process in which personal data from two or more sources is combined to create a "mosaic" of individuals that would not be discernable from the individual pieces of data alone.
Data Matching	A technique in which two or more unrelated pieces of personal information are cross-referenced and compared to generate a match, or "hit, " that suggests a person's connection with two or more groups.
Data Mining	A technique for "unearthing" implicit patterns in large single databases, or "data warehouses," revealing statistical data that associates individuals with nonobvious groups; user profiles can be constructed from these patterns.

3.9 Protecting Personal Privacy in Public Space

So far, we have examined how cybertechnology can be used to gather, exchange, and mine personal information. With the exception of data mining, which manipulates personal, but nonconfidential information, the kind of personal information gathered and exchanged was often confidential and intimate in nature. This confidential and very personal information is referred to as nonpublic personal information (NPI).

Privacy analysts are now concerned about a different kind of personal informationpublic personal information (PPI), which is neither confidential nor intimate and which is also being gathered, exchanged, and mined using cybertechnology. PPI includes information about you, such as where you work or attend school or what kind of car you drive. Even though it is information about you as a particular person, PPI has not enjoyed the privacy protection that has been granted to NPI.

Nissenbaum (2004b) believes that many in the commercial sector proceed from an assumption that she believes is erroneousviz., There is a realm of public information about persons to which no privacy norms apply.

Because the information I have acquired about you in the above scenario can be considered public information, it would not warrant any legal privacy protection. And even though this information is about you as a person, it is not the kind of personal information to which we, as a society, would typically grant normative privacy protection.

Now we can see why some people worry about having their movements online tracked and recorded. The information gathered about you is, in effect, the collector's information, even though it pertains to you as a person; the collector now owns that information about you, as well as the information it has about its other customers, and is, in principle at least, free to do with that information whatever it chooses. On the one hand, the information seems fairly innocuousafter all, who really cares which books you happen to browse or purchase? On the other hand, however, this information can be combined with other information about your online transactions at additional Web sites to create a consumer profile of you, which can then be sold to a third party.

One argument that online entrepreneurs might advance to defend these business practices is that if a user puts information about him- or herself into the public domain of the Internet, then that information is no longer private. Of course, one response to this line of reasoning could be to question whether users clearly understand the ways that data they submit might subsequently be used. Corporation used information about you in ways that yo u neither authorized nor intendedan example of the kind of practice that Nissenbaum (2004a, 2010) describes as violating contextual integrity.

3.9.1 Search Engines and the Disclosure of Personal Information

Internet search engines are valuable for directing us to available online resources for academic research, commerce, recreation, and so forth; yet search engine technology, too, can be controversial from the perspective of personal privacy.

At least two different kinds of concerns affecting privacy arise because of practices involving search engines: (1) search engine companies such as Google record and archive each search request made by users and (2) search engines enable users to acquire a wealth of personal information about individuals, with relative ease.

It is not only the fact that an individuals search requests are recorded and archived by major companies such as Google that make Internet search engines controversial from the perspective of personal privacy. Search engine-related privacy issues also arise because that technology can be used for questionable purposes such as stalking.

Consider the amount and kind of personal information about ordinary individuals that is now available to search engines. In some cases, that information may have been placed on the Internet inadvertently, without the knowledge and consent of those affected. Yet information about those persons can be located by an Internet user who simply enters their names in a search engine programs entry box. The fact that one can search the Internet for information about someone might not seem terribly controversial. After all, people regularly place information about themselves on Web sites (or perhaps they authorize someone else to do it for them) and on social networking services such as Facebook and LinkedIn. And it might seem reasonable to assume that any online personal information that is currently available to the public should be viewed simply as public information. But should such information about persons be unprotected by privacy norms merely because it is now more easily accessible for viewing by the public?

We have seen how the use of search engines can threaten the privacy of individuals in two distinct ways: (1) by recording and archiving records of a users search queries that reveal the topic of the search and the time the request was made by the user and (2) by providing users of search engines with personal information about individuals who may have no idea of the wealth of personal information about them that is available online (and have no control over how it is accessed and by whom it is accessed). The latter concern is further complicated by the fact that individuals who are the subject of online searches enjoy no legal protection because of the presumed public nature of the personal information about them that is available via online searches.

3.10 Accessing Online Public Records

Another kind of personal information that can also be considered public in nature is information about us stored in records located in municipal buildings, which are accessible to the general public. Public records have generally been available to anyone willing to go to those municipal buildings and request hardcopy versions of them. Some municipalities charge a small fee to retrieve and copy the requested records. Many of these public records can now also be accessed online. Has this changed anything?

Consider that information merchants were always able to physically or manually collect all of the public records they could acquire. But traditional information entrepreneurs without computer technology would have had to hire legions of clerks to collect the (publicly available) data, sort the data according to some scheme, and then compile and print the data for sale. The process would have been physically impractical and hardly profitable, given the labor it involved; it would probably never have occurred to anyone even to attempt it prior to the advent of sophisticated information technology.

We could ask why public records were made public in the first place. Were they made public so that information merchants could profit from them, or were they instituted to serve broader societal and governmental ends? In order for governmental agencies at all levels to operate efficiently, records containing personal information are needed.

It has been assumed that the availability of public records causes no harm to individuals, and that communities are better served because of the access and flow of those records for what seems to be legitimate purposes. But information gathering companies now access those public records, manipulate them to discover patterns useful to businesses, and then sell that information to third parties.

Many information merchants seem to assume that offices responsible for maintaining public records now have a legal obligation to make all public records available online. Their presumption is that the government has no right to restrict or limit, in any way, information that has been deemed appropriate for inclusion in public records. Is this a reasonable presumption?

We ask again, What was the purpose of making such records public in the first place? There is no reason to believe that it was to facilitate commerce in the private sector. Of course, selling information, as the State of Oregon did, is now an important source of revenue for many state governments. But we also need to consider the privacy (and other ethical) implications of states selling information about their residents to online merchants, especially in an era where technology makes it so easy to erode personal privacy. Can technology also provide us with tools to protect our privacy?

3.11 Privacy-enhancing Technology

We have seen how cybertechnology has exacerbated privacy concerns. Ironically, perhaps, cybertechnology also provides tools that can help users to protect their privacy. For example, privacy-enhancing technologies or PETs have been developed to help users protect (a) their personal identity while navigating the Internet and (b) the privacy of their online communications (such as e-mail). An example of (b) is encryption tools that encode and decode e-mail messages. Our main focus in this section is on whether PETs actually

accomplish (a).
Some PETs enable users to navigate the Internet either anonymously or pseudonymousl y;It is important to note that although Anonymizer users enjoy anonymity while visiting Web sites, they are not an onymous to Anonym izer.c om or to th eir own ISPs. A user s activiti es on a Web site can be recorded in server log files and can thus be traced back to a specific ISP and IP address. To enjoy complete anonymity on the Internet, online users need tools that do not require them to place their trust in a single third party".
Although PETs assist users in navigating the Web with relative anonymity, they are not useful for e-commerce transactions in which users must reveal their actual identities. Many e-commerce sites now provide users with a stated privacy policy that is backed by certified trustmarks or trust seals (discussed in more detail in Section 5.9.1). These trust agreements between users and e-commerce sites can also be viewed as PETs in that they are intended to protect a users privacy during a consumer transaction. But are they adequate to the task?

3.11.1 Educating Users about PETs

How are users supposed to find out about PETs? Consider that Web sites are not required to inform users about the existence of PETs or to make those tools available to them. Furthermore, online consumers must not only discover that PETs are available, but they must also learn how to use these tools. So at present, responsibility for learning about PETs and how to use them is incumbent upon consumers. Is it reasonable and is it fair to expect users to be responsible for these tasks?
Why not further presume that users do not want their personal data used in ways they did not explicitly authorize when they initially disclosed it in a commercial transaction? Following Judith DeCew (2006), we could presume in favor of privacy and then develop ways that would allow individuals to determine for themselves how and when that presumption should be overridden. (This is part of a process that DeCew refers to as dynamic negotiation.) Independent of questions about where the presumption should reside, however, the widespread application and use of PETs will require a massive educational effort.

3.11.2 PETs and the Principle of Informed Consent

Even if the consumer-education-related issues involving PETs can be resolved, other questions need to be asked. For example, do PETs adequately support users in making *informed* decisions about the disclosure of their personal data in commercial transactions? Traditionally, the principle of informed consent has been the model, or standard, in contexts involving the disclosure of ones personal data. However, users who willingly consent to provide information about themselves for one purpose (e.g., in one transaction) may have no idea how that information can also be used in secondary applications.
Some in the commercial sector argue that because no one is forcing users to reveal personal data, the disclosure of such data is done on a completely voluntary basis. Assume that a user has willingly consented to disclose personal data in an e-commerce transaction. Has the user also consented to having that information used for additional, secondary purposes?

Recall our discussion in Section 5.6 about data mining, where we saw that specific information given by a consumer for use in one context could be subsequently mined.
We can also ask whether businesses that collect personal data could possibly know in advance exactly how those data will be used in secondary and future applications? When data mining technology is involved, for example, it would seem that businesses could not adequately inform users about exactly how their personal data might be used in secondary applications. What kind of informed choice, then, could users make in these cases?
Some in the e-commerce sector have responded to critics by pointing out that in most cases, users are provided with the means to either opt-in or opt-out of having their personal data collected, as well as having those data made available for secondary use. But the default is such that if no option is specified by the user when he or she discloses personal data for use in one context, then those disclosed personal data are also available for secondary use. Hence, the policy is presumed consent, not informed consent. Is that presumption fair to online consumers?
Because PETs provide users with some ways of protecting their identity and also provide them some choice in controlling the flow of their personal information, they would seem to be an empowering rather than a disabling technology. But PETs alone are insufficient for resolving many privacy concerns affecting e-commerce.

3.12 Privacy Legislation and Industry Self-regulation

We saw in the previous section that even though PETs offer users a means to protect their identity in certain kinds of activities, they are not the magic bullet many of their staunchest supporters have suggested. Recognizing the limitations of PETs, some privacy advocates believe that stronger privacy laws will protect consumers, whereas others in the commercial sector, for example, believe that additional privacy legislation is neither necessary nor desirable. Instead, they suggest strong industry controls regulated by standards.
Generally, privacy advocates have been skeptical of voluntary controls, including industry standards for self-regulation initiatives. Instead, they argue for stricter privacy legislation and data protection principles to protect the interests of users. We begin this section with a look at certain self-regulatory schemes for privacy protection that is provided to consumers by industry standards.

3.12.1 Industry Self-regulation Initiatives Regarding Privacy

Some industry representatives who advocate for the use of voluntary controls might concede that tools such as PETs, in themselves, are not adequate to protect the privacy of consumers in e-commerce transactions. However, they also believe that alternatives to additional privacy legislation are possible. These advocates point to the establishment of industry standards that have already been accepted and implemented. Some of these standards are similar to PETs in the sense that they are intended to protect a users privacy, but unlike PETs in that they are not themselves tools.
An industry-backed (self-regulatory) initiative called TRUSTe was designed to help ensure that Web sites adhere to the privacy policies they advertise. TRUSTe uses a branded system of trustmarks (graphic symbols), which represent a Web sites privacy policy

regarding personal information. Trustmarks provide consumers with the assurance that a Web sites privacy practices accurately reflect its stated policies. Through this PET-like feature, users can file a complaint to TRUSTe if the Web site bearing its trust seal does not abide by the stated policies. Any Web site that bears the TRUSTe mark and wishes to retain that seal must satisfy several conditions: The Web site must clearly explain in advance its general information-collecting practices, including which personally identifiable data will be collected, what the information will be used for, and with whom the information will be shared. Web sites that bear a trust seal but do not conform to these conditions can have their seal revoked. AndWeb sites displaying trust seals, such as TRUSTe, are subject to periodic and unannounced audits of their sites. Critics have pointed out some of the difficulties in implementing TRUSTe. For example, the amount of information users are required to provide can easily discourage them from carefully reading and understanding the agreement. Also, the various warnings displayed may appear unfriendly and thus might discourage users; friendlier trustmarks, on the contrary, might result in users being supplied with less direct information that is important for protecting their privacy. But advocates of tools such as TRUSTe argue that, with these tools, users will be better able to make informed choices regarding electronic purchasing and other types of online transactions.

The Toysmart incident illustrates a situation in which users had exercised control over their personal information in one contextthat is, in electing whether to disclose information about themselves to Toysmart in online transactionsbased on specific conditions stated in Toysmarts privacy policy. However, it also turned out that these individuals were not guaranteed that the personal information they disclosed to Toysmart would be protected in the future. Thus, it would seem that controls beyond those provided by trustmarks and e-commerce vendors are needed.

Another concern has to do with various privacy policies established by search engine companies. Unlike e-commerce sites, which users can easily avoid if they wish, virtually every Internet user depends on search engines to navigate the Web. We saw how major search engine companies such as Google record and keep a log of users searches. This practice, as we also saw, has generated privacy concerns. Because of concerns involving distrust of Google and other commercial Web sites to regulate themselves, privacy advocates believe that explicit privacy laws are needed to protect users. We next briefly examine some existing privacy legislation.

3.13 Privacy Laws and Data Protection Principles

So far, we have considered various kinds of proposals aimed at addressing privacy concerns. Some have called for stricter privacy laws on the part of governments and for the formation of privacy oversight commissions to enforce those laws. Others call for more serious self-regulatory measures by those in the commercial sector. And some proposals have suggested the need for technological solutions that empower online users by providing them with privacy-enhancing tools. Can these various proposals, or at least relevant aspects of them, be successfully combined or integrated into one comprehensive proposal?

While there has been no uniform consensus on a comprehensive privacy policy, especially one that could be implemented across international borders, there does seem to be

considerable agreement on at least one point: any comprehensive privacy policy should be as transparent as possible. In examining James Moors theory of privacy in Section 5.2.4, we saw that personal privacy could be protected in situations or zones that were declared normatively private. We also saw that Moor requires that the rules for setting up normatively private situations be public and open to debate. This point ismade explicit in his Publicity Principle, which states that the rules and conditions governing private situations should be clear and known to persons affected by them (Moor 2000). Thus, a critical element in Moors model for an adequate privacy policy is openness, or transparency, so that all parties in the situation, or context, are kept abreast of what the rules are at any given point in time. In this sense, Moors publicity principle would seem to provide a key foundational element in any comprehensive privacy policy that incorporates legislation, self-regulation, and privacy-enhancing tools.

4 Cybercrime and Cyber-Related Crimes

4.1 CyberCrime and Cybercriminals

4.1.1 Background Events: A Brief Sketch

By the turn of the twenty-first century, there was a growing concern in both the private and the public sectors that no types of activities leading to unauthorized access should be tolerated. Perhaps this change in sentiment is due to our societys increased dependence on networked computers and the Internet.
Of course, unauthorized break-ins are only one of the many kinds of crimes made possible by computers and cybertechnology. Richard Power (2000), who believes that most computer crimes involve either fraud or abuse, or both, distinguishes between the two notions in the following way:
He identifies *computer fraud* as computer-related crimes involving deliberate misrepresentation or alteration of data in order to get something of value; he defines *computer abuse*, on the contrary, as willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Power notes that these abuses can include embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation.
Analysts believe that many cybercrimes go unreported. Wall (2007) notes that in at least some cases, organizations are reluctant to report cybercrimes because of the embarrassment it might cause them. Other analysts believe that many of these crimes go unreported because the victims fear the negative repercussions: reporting the crimes would be tantamount to admitting that their computer security practices are inadequate.

4.1.2 A Typical Cybercriminal

Parkers classic study suggested that we should carefully distinguish between hackers who commit crimes, i.e., as people who are primarily nonprofessional or amateur criminals, and "professional criminals."" He believes that stereotypical computer hackers, unlike most professional criminals, are not generally motivated by greed; some seem to thrive on a kind of joyriding (the thrill experienced in figuring out how to break into unauthorized systems). Along somewhat similar lines, Sagiroglu and Canbek (2009) point out that in the early days of computing, idealistic hackers were inclined to attack computers merely to prove that they could or to show off to one another. Characteristics such as these would seem to differentiate many traditional hackers from professional criminals.
Although many malicious hackers are considered amateur criminals, some possess an expertise with computers comparable to that of the best technical experts in computer science. However, it is also worth noting that many malicious hackers do not possess outstanding technical skills but are savvy enough to locate sophisticated hacking tools that can be downloaded from the Internet for free, and many of these individuals are sufficiently astute to take advantage of holes in computer systems and programs. Michael Simpson (2006) notes that these individuals, who tend to be young and inexperienced, are sometimes referred to by sophisticated computer programmers as script kiddies or packet monkeys, because they copy code from knowledgeable programmers as opposed to creating

the code themselves.

4.2 Defining Cybercrime

Gotterbarns position can be interpreted in a way to suggest that no distinct category of computer crime or cybercrime is needed. Stephane Leman-Langlois (2008) makes a similar suggestion in stating that cybercrime, or what she calls "technocrime," does not exist." In Leman-Langlois view, cybercrime "is simply a convenient way to refer to a set of concepts...shaping the ways we understand matters having to do with the impact of technology on crime, criminals and our reactions to crimeand vice versa."
We next take up the question of criteria for distinguishing computer/cyber crimes from other kinds of crimes. In particular, we ask whether the criteria used by lawmakers to frame various categories of computer crime or cybercrime been coherent.

4.2.1 Framing a Coherent and Comprehensive Definition of Cybercrime

Recall our discussion in Chapter 1 of James Moors insight that computer technology is logically malleable and thus creates new possibilities for human action. We saw that these new possibilities, in turn, sometimes generate both policy vacuums and conceptual muddles (Moor 2007). By extension, these new possibilities for human action include new possibilities for crime. Many of these possibilities have resulted in criminal actions that have forced us to stretch traditional concepts and laws dealing with crime. Applying Moors insight, we can further ask whether any new forms of crime have been made possible by cybertechnology. If we answer yes, then some crimes may be unique to computers and cybertechnology.
By thinking about cybercrimes in terms of their unique or special featuresi.e., conditions that separate them from ordinary crimeswe could distinguish authentic or genuine cybercrimes from other crimes that merely involve the use or the presence of cybertechnology. We propose a definition of a genuine cybercrime as a crime in which

the criminal act can be carried out only through the use of cybertechnology and can take place only in the cyberrealm.

4.3 Three Categories of Cybercrime: Piracy, Trespass, and Vandalism in Cyberspace

Using our definition of cybercrime, we can further categorize genuine cybercrimes as follows:

1. Cyberpiracyusing cybertechnology in unauthorized ways to
   (a) reproduce copies of proprietary information, or
   (b) distribute proprietary information (in digital form) across a computer network.
2. Cybertrespassusing cybertechnology to gain unauthorized access to
   (a) an individuals or an organizations computer system, or

(b) a password-protected Web site.

3. Cybervandalismusing cybertechnology to unleash one or more programs that

   (a) disrupt the transmission of electronic information across one or more computer networks, including the Internet, or

   (b) destroy data resident in a computer or damage a computer systems resources, or both.

If our model is correct, then many crimes that use cybertechnology are not genuine cybercrimes. For example, crimes involving pedophilia, stalking, and pornography can each be carried out with or without computers and cybertechnology; there is nothing about them that is unique to cybertechnology, so crimes such as Internet pedophilia, cyberstalking, and Internet pornography would not qualify as genuine cybercrimes. (We will see below that they are examples of cyber-related crimes.)
Using our definition of cybercrime, there is no need to consider motive, political cause, ideology, etc., when determining how the criminal acts best fit into one of our three categories. (However, motive or intention could influence the ways that cybercrimes are prosecuted and that convicted cybercriminals are sentenced.)

4.4 Cyber-Related Crimes

Cyber-related crimes can, in turn, be divided into two subcategories: *cyberexacerbated* crimes and *cyberassisted* crimes. This distinction enables us to differentiate between a crime in which someone merely uses cybertechnology (e.g., a personal computer to file a fraudulent income tax return) from crimes such as Internet pedophilia and cyberstalking, which are significantly affected by computers and cybertechnology. The role that cybertechnology plays in the first example seems at best trivial and possibly altogether irrelevant, but in the latter two examples, cybertechnology does much more than merely *assist* someone in carrying out a crimecybertechnology *exacerbates* the crimes.

4.4.1 Some Examples of Cyber-Exacerbated vs. Cyber-Assisted Crimes

Certain kinds of crimes aided by cybertechnology can increase significantly because of that technology. For example, in the case of cyberexacerbated crimes, the scale on which crimes of a certain type can be carried out is significantly affected. Consider the potential increase in the number of stalking-, pornography-, and pedophilia-related crimes that can now occur because of cybertechnology, vs. the likely increase in the number of income tax crimes, which are also assisted by computer technology.
Along lines that are somewhat similar to the distinctions we have drawn in separating three categories of cybercrime-cyberassisted, cyberexacerbated, and cyberspecific (or genuine cyber) crimes-Wall (2007) proposes the following scheme based on three "generations" of cybercrime.
What we call cyberassisted crimes, he describes as first generation cybercrimes that are, in effect, traditional or ordinary crimes that happen to involve the use of a computer.
Corresponding to our category of cyberexacerbated crimes is Walls notion of second

generation or hybrid crimes. For this set of cyber-related crimes, Wall points out that network technology has created entirely new global opportunities.
His third generation of cybercrimes comprises a category that Wall calls true cybercrimes, which corresponds to our category of genuine cybercrimes in that they are solely the product of the Internet(or, in our case, the product of cybertechnology).
Wall notes that in the case of cybercrimes involving the first two generations, individuals and organizations could still find ways of carrying out the criminal activities in the event that either the computer or the Internet was eliminated. In the case of true cybercrimes, however, Wall points out that if you eliminate the Internet, those crimes vanish. He uses the examples of spamming and phishing to illustrate this point. These examples complement the set of crimes we identified above as genuine cybercrimes.
Figure below illustrates some ways in which crimes involving the use of cybertechnology can be catalogued according to this threefold scheme.

We should not underestimate the significance of many cyber-related crimes, even if they

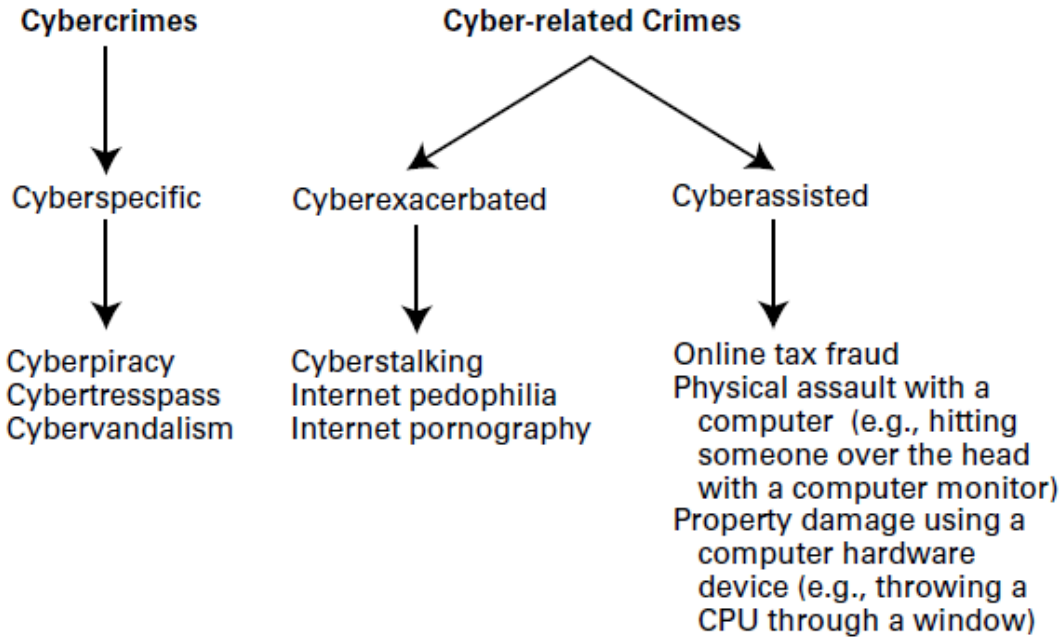


Figure 3: Cybercrimes and cyber-related crimes

fail to qualify as genuine or true cybercrimes. Consider that some cyber-related crimes, including cyberstalking and cyberbullying, have resulted in deaths.
Although the authors of both books suggest that there may be some aspects of cyberstalking (vs. offline stalking) crimes and cyberbullying (vs. traditional bullying) crimes, respectively, that challenge our conventional laws, neither succeeds in making a convincing case for why those criminal acts should qualify as examples of what we call genuine cybercrimes. But, in describing the many ways that stalking and bullying crimes have increased significantly because of cybertechnology, the authors make a very strong case for why those cyber-related crimes would qualify as cyberexacerbated crimes rather

than merely cyberassisted crimes.

4.4.2 Identity Theft

What is identity theft, and how is it exacerbated by cybertechnology? Lininger and Vines (2005) define identity theft as

> a crime in which an imposter obtains key pieces of personal information, such as social security or drivers license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials.

Identity-theft crimes can also include the taking of another persons identity through the fraudulent acquisition of personal information in credit card numbers. However, Wall (2007) notes that identity theft is often mistakenly used to describe crimes involving credit card theft. So, not all instances of the latter kind of theft qualify as identity theft.

Of course, identity theft, like other cyber-related crimes, does not require cybertechnology. But identity thieves have been very successful in scams involving cybertechnology in general (e.g., in recording credit card swipes), independent of the Internet per se.

Factors such as lax security and carelessness involving customer information contained in computer databases and in company-owned laptop computers has made it easy for some identity thieves to acquire personal information about their victims.

As we saw in Chapter 5, information merchants purchase and sell personal information, including social security numbers and credit card information. And many are willing to pay for this information. So information brokering has become a lucrative business, and this has not gone unnoticed by professional criminals as well as by some employees in organizations that have access to sensitive information about peoples financial records.

Many kinds of identity-theft scams have also been carried out on the Internet. One common example is a scheme involving e-mail that appears to have been sent by a reputable business.

Many e-mail messages sent from identity thieves are generated through spam (examined in Chapter 9). Using spam to gather personal information is sometimes referred to as phishing, which Lininger and Vines (2005) describe as automated identity theft. They point out that phishing "combines the power of the Internet with human nature to defraud millions of people out of billions of dollars." They also believe that phishing may soon overtake spam as the main Internet headache. Lininger and Vines cite a study by the Anti-Phishing Working Group (APWG), which reports that the number of phishing incidents is increasing at a rate of about 56% per month.

An automated version of phishing, sometimes called pharming, automatically redirects the victim to the offending site (Wall 2007). Activities involving pharming and phishing, along with conventional e-mail spam, increase the amount of identity theft that can be accomplished over the Internet. And we have seen how other, non-networked uses of cybertechnology also exacerbate identity-theft crimes.

5 Security in Cyberspace

5.1 Security in the Context of Cybertechnology

Securityespecially, in the context of computing and cybertechnologyhas no universally agreed-upon definition. The expressions *computer security* and *cybersecurity* are often associated with issues having to do with the reliability, availability, and safety, of computers systems, as well as with the integrity, confidentiality, and protection of data. Richard Epstein (2007) suggests that security concerns affecting computers and cybertechnology can be viewed in terms of three key elements:

- confidentiality,
- integrity,
- accessibility

Whereas confidentiality is about preventing unauthorized persons from gaining access to unauthorized information, integrity, in computer security contexts, is about preventing an attacker from modifying data. In Epsteins scheme, accessibility has to do with making sure that resources are available for authorized users."
Are any additional elements or criteria useful for understanding cybersecurity? Peter Neumann (2004) notes that, in addition to providing desired confidentiality, integrity, and accessibility, cybersecurity aims at preventing misuse, accidents, and malfunctions with respect to computer systems. Neumann also notes, however, that cybersecurity can be a double-edged sword; for example, it can be used to protect privacy, but it can also be used to undermine freedom of access to information for users.
In defining cybersecurity, it is important to point out that sometimes issues involving security in cyberspace overlap with concerns pertaining to cybercrime; other times they intersect with issues involving privacy.

5.1.1 Cybersecurity as Related to Cybercrime

While most intentional cybersecurity violations are illegal and often criminal, not every crime in cyberspace involves a breach, or violation, of cybersecurity.
Consider three cyber-related crimes that have no direct implications for cybersecurity: a pedophile can use a computer to solicit sex with young children, a drug dealer can use the Internet to traffic in drugs, and a student can use an electronic device to pirate copyrighted music. Although each of these activities is clearly illegal, it is not clear that any of them necessarily result from insecure computers. Perhaps greater security mechanisms on computer networks could deter crimes and detect criminals in cyberspace, but cyber-assisted crimes involving pedophilia, drug trafficking, and pirating music do not typically result from security flaws in computer system design. There are, then, important distinctions between issues of security and crime involving cybertechnology.
Just as cybersecurity issues are sometimes lumped together with cybercrime, security concerns involving cybertechnology can also overlap with worries about personal privacy.

5.1.2 Security and Privacy: Some Similarities and Some Differences

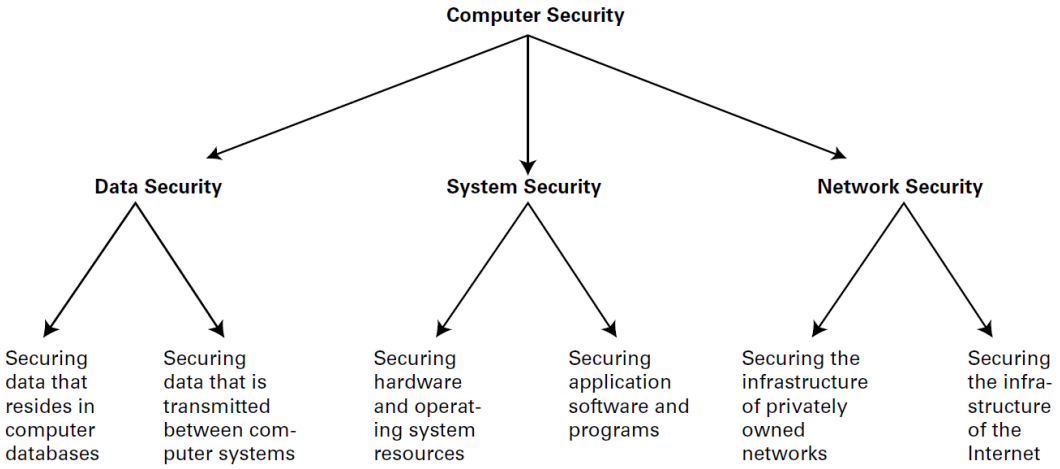
The concepts of privacy and security are not always easy to separate, especially when civil liberties and basic human rights are discussed. Paul Thompson (2001) believes that many of our claims involving a right to privacy are grounded in the notion of security and can be better understood as arguments concerning a "right to being secure."

Although cyber-related issues involving privacy and security can overlap, some important distinctions are nonetheless worth drawing. Privacy concerns affecting cybertechnology often arise because people fear losing control over personal information that can be accessed by organizations (especially businesses and government agencies), many of whom claim to have some *legitimate* need for that information in order to make important decisions. Security concerns, on the contrary, can arise because people worry that personal data or proprietary information, or both, could be retrieved and possibly altered, by unauthorized individuals and organizations.

Privacy and security concerns can be thought of as two sides of a single coin: People need personal privacy and they wish to control those who have information about them as well as how that information is accessed by others. Making sure that personal information stored in computer databases is secure is important in helping them achieve and maintain their privacy. In this sense, then, the objectives would seem compatible with, and even complementary to, security. In another sense, however, there is a certain tension between privacy and security. From the perspective of security, the protection of system resources and proprietary data is generally considered more critical, whereas from the vantage point of privacy, the protection of personal information and personal autonomy will receive a higher priority.

In analyzing the tension involving privacy vs. security interests, Kenneth Himma (2007a) has argued that threats to security outweigh comparable threats to the right to privacy. On the contrary, Helen Nissenbaum (2010) offers a more sympathetic appeal to the value of privacy in her analysis of the trade-offs between the two competing interests. The following quotation, attributed to Ben Franklin (17061790), is sometimes cited by privacy advocates to express their interpretation of what is at stake in the dispute involving security vs. privacy interests: They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety. However, in an era where concerns about cyberterrorism now influence our public policy debate, many people may be more willing to give up aspects of their liberty and privacy for greater security.

In the context of cybersecurity, privacy-related concerns include protecting personal data from unauthorized access, abuse, and alteration, and thus reflect values that preserve individual autonomy and individual respect for persons. And while anonymity tools help to protect the privacy of individuals navigating in cyberspace, those tools can also cause serious concerns for security because anonymous behavior makes it difficult to identify security violators. So, in some cases, there is a natural tension between security and privacy, as we have seen; at other times, however, the objectives and goals of privacy and securityfor example, with respect to confidentiality and data integrityare the same.



5.2 Three Categories of Cybersecurity

Security issues involving cybertechnology span a range of concerns having to do with three distinct kinds of vulnerabilities:

i Unauthorized access to *data*, which are either resident in or exchanged between computer systems.

ii Attacks on *system resources* (such as computer hardware, operating system software, and application software) by malicious computer programs.

iii Attacks on *computer networks*, including the infrastructure of privately owned networks and the Internet itself.

We refer to the first of these three categories of security concerns as data security. The second category of concerns can be described under the heading system security, and the third can be understood as network security..

5.3

Data Security is concerned with vulnerabilities pertaining to unauthorized access to data. Those data can either (a) reside in one or more computer storage devices or (b) be exchanged between two or more computer systems, or both. In particular, data security issues affect the confidentiality, integrity, and availability of information. Richard Spinello (2000) aptly describes what is required for data security when he points out that

> ...proprietary or sensitive information under ones custodial care is kept confidential and secure, that information being transmitted is not altered in form or content and cannot be read by unauthorized parties, and that all information being disseminated or otherwise made accessible through Web sites and online data repositories is as accurate and reliable as possible

Three points in this description are worth highlighting. First, the information to be protected can be either *proprietary* or *sensitive*, or both. (Proprietary information, as we

will see, is legally protected by schemes such as copyrights and patents and thus can be owned by corporations or by individuals, while sensitive information is generally considered to be intimate or confidential because it includes personal, medical, and financial records.)
Second, the information must be secured not only from tampering and alteration by unauthorized parties but also from merely being accessed (and read) by those parties.
Third, and finally, the stored information must be accurate, readily available, and accessible to authorized parties. So, not only must the information residing in a computer database or in a password-protectedWeb site be available at optimal times, it must be able to be accessed by authorized users at any timei.e., accessible on demand.
Data security is now also threatened by cloud-computing services, as more and more corporations and ordinary users elect to store their data in the Cloud. Cloud storage devices provide users with one means to secure their data by ensuring that their data could survive (a) crashes on the hard drives of their personal computers, and (b) physical damages involving their electronic tablets and electronic devices. However, cloud storage also poses a threat to data security because unauthorized users could gain access to, and potentially manipulate, personal data that is stored there.

5.3.1 System Security: Viruses, Worms and Malware

System security is concerned with vulnerabilities to system resources such as computer hardware, operating system software, and application software. As such, it is concerned with various kinds of viruses, worms, and related malicious programs that can disrupt and sometimes destroy computer systems. What are the differences between computer viruses and worms? According to Ed Skoudis (2004), a virus is a self-replicating piece of software code that attaches itself to other programs and usually requires human action to propagate. He defines a worm in contrast as a self-replicating piece of code that spreads via networks and usually doesnt require human interaction to propagate. Michael Simpson (2006) points out that worms replicate and propagate without needing a host or program.
Some security analysts differentiate further between the two types of disruptive programs by pointing out that a worm is less virulent than a virus. However, worms can spread more quickly than viruses, because worms, unlike viruses, do not need any human action to trigger them. We already noted that viruses cannot run on their own and are often activated when an unsuspecting user opens an e-mail attachment. Worms, on the contrary, can move from machine to machine across networks and can have parts of themselves running on different machines.
Simpson (2006) notes that malware can take many forms and can also include spyware. The effects of malware can range from minor annoyances with individual computer systems, to preventing an entire organization from operating, to shutting down computer networks, to disrupting major segments of the Internet.

5.3.2 Network Security: Protecting our Infrastructure

A third category of computer security, which we call *network security*, is concerned with securing computer networksi.e., from privately owned computer networks (such as LANs and WANs) to the Internet itselfagainst various kinds of attacks. The Internets infrastructure

has been the victim of several attacks. These attacks have ranged from programs launched by individuals with malicious intentions to individuals who claimed their intentions were benign. In many cases, these attacks have severely disrupted activities on segments of the Internet. In a few cases, they have also rendered the Internet virtually inoperable.
Because many nations now depend on a secure cyberspace for their physical infrastructures, including power grids, there has been increased concern over threats from international hacking groups, including governments and state-sponsored organizations.

Cybersecurity Category	Corresponding Area(s) of Concern
Data security	Concerned with vulnerabilities pertaining to unauthorized access to *data*, as well as with threats to the confidentiality, integrity, and availability of data that resides in computer storage devices or is exchanged between computer systems.
System security	Concerned with attacks on *system* resources (such as computer hardware, operating system software, and application software) by malicious programs.
Network security	Concerned with attacks on computer *networks*, including the infrastructure of privately owned networks as well as the Internet itself.

5.4 Hacking, Cracking and Counterhacking

Pekka Himanen (2001) notes that hacker originally meant anyone who programmed enthusiastically and who believed that information sharing is a powerful positive good. The hacker Jargon File (maintained on the Web by Eric Raym ond at www .tuxedo.org/ esr/jarg on) defines a hack er as an expert or en thusiast of an y kind. Note that, a ccording to this de finiti on, a hacker need not be a computer enthusiast; for example, someone could be an astronomy hacker. In fact, a hacker, in the generic sense of the term, might have no interest in computers or cybertechnology at all.

5.4.1 Hacking vs. Cracking

Himanen points out that the meaning of hacker began to change in the 1980s when the media started applying the term to criminals using computers. In order to avoid confusion with virus writers and intruders into information systems, traditional hackers began calling these destructive computer users crackers. According to the hacker Jargon File, a cracker is one "who breaks security on a system". Crackers often engage in theft and vandalism once they have gained access to computer systems.
Some authors, including Wall (2007), also use the expressions white hat and black hat to distinguish between the two types of hacking behavior. The phrase white hat hackers is used to refer to those innocent, or nonmalicious, forms of hacking, while black hat hackers refers roughly to what we described above as cracking. However, distinctions between hacking and cracking, and between white-hat and black-hat hackers, are generally not recognized

and observed in the world beyond the computer community. So the media often refers to crackers, or black hat hackers, simply as hackers. This, in turn, has perpetuated the negative image of hackers and hacking in society at large.

5.4.2 Active Defense Hacking: Can Acts of "Hacking Back" or Counter Hacking Ever Be Morally Justified?

Amore recent controversy associated with hacking activities has to do with active defense hacking, sometimes also referred to as counter hacking or hacking back against hackers. Counter hacking activities have been carried out both by individuals and corporations; they are directed against those who are suspected of originating the hacker attacks. In some cases, counter hacking has been pre-emptive; in other cases, it has been reactive. Both forms are controversial, but pre-emptive counter hacking is arguably more difficult to defend.

we saw that at least one organization offers a certification program to train ethical hackers. Individuals who successfully complete this programi.e., Certified Ethical Hackersare trained and certified not only in the use of defensive measures to ensure the security of their employers, but also appear to be authorized to engage in security-related activities that involve pre-emptive strikes as well. According to the Certified Ethical Hacker Web site:

> The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits . . . an Ethical Hacker is very similar to a Penetration Tester . . . When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal.

But is it, or should it be, legal to engage in pre-emptive hacking attacks? Some who defend pre-emptive acts of counter hacking believe that they can be justified on utilitarian, or consequentialist, grounds. For example, they argue that less overall harm will likely result if pre-emptive strikes are allowed. However, it would seem that many of the same difficulties that arose in applying a utilitarian justification for computer break-ins in extraordinary cases (examined in Chapter 6) also arise in the case of extending a utilitarian argument to defend counter hacking in its pre-emptive form.

Because counter hacking can cause harm to innocent individuals, we can question whether this practice can be defended on moral grounds. Kenneth Himma (2004, 2008) points out that in the case of hacking back against those who launch DDoS attacks, many innocent persons are adversely affected because the attacks are routed through their computer systems. As we noted in Chapter 6, perpetrators of DDoS attacks use host computers, which often include the computers of innocent persons, to initiate their attacks (a technique sometimes referred to as IP spoofing). This would suggest to the victims of these attacks that they originated from the host computer, as opposed to the computer of the initiator of the attack. So when victims hack back, they can unintentionally cause the intermediate computer to be assaulted.

So, even if utilitarian arguments showed that counter hacking resulted inmore desirable outcomes for the majority of society, deontologists (and other nonconsequentialists) would argue that such practices are morally unacceptable if they do not respect the rights of innocent individuals. In this case, those individuals would be unfairly used as a means to

an end, which, as we saw in Chapter 2, is not permissible in deontological ethical theories. It is difficult to provide a moral justification for counter hacking; and from a legal perspective, it is not clear whether hacking back can be viewed in a way that is not criminal. For example, if hacking is illegal, then it would seem that hacking back would be no less illegal. However, until a case of counter hackingespecially one that involves a pre-emptive attack in the form of a DDoSis officially tried in court, it is difficult to say how our legal system will respond.

6 Regulating Commerce and Speech in Cyberspace

Many conservative organizations have argued for censorship of certain kinds of speech in cyberspace. Some liberal groups, on the contrary, who oppose any restrictions on free speech in cyberspace, argue that e-commerce, not speech, needs to be regulated. In this chapter, we consider speech to include issues involving pornography, hate speech, and speech that can cause physical harm to others. And somewhat more loosely, we consider e-commerce regulation issues to include concerns involving electronic spam, the assignment of Internet domain names, and practices affecting hyperlinking on the Web.
We will also see why we should be concerned about cyberspace regulation that can be implemented with technology itself, by means of regulation by code, as in the case of Digital Rights Management(DRM) technologies. Some critics worry that regulation by code is becoming the default regulatory scheme in cyberspace.

6.1 Background issues and some preliminary distinctions

John Weckert (2007) believes that when discussing cyberspace regulation, we need to ask two separate questions:

A *Can* it be regulated?

B *Should* it be regulated?

Asking question (A) implies that it is not clear whether cyberspace can be effectively regulated, but we will operate on the assumption that it can, in fact, be, regulated. We also acknowledge, however, that regulation schemes can be difficult to implement and enforce, and we concede that regulation can have undesirable side effects in terms of both cost and efficiency.
We will focus on question (B), that is, the normative question as to whether cyberspace ought to be regulated. This question also can be broken down into two separate questions, as Weckert points out when he asks: "Should it be regulated in general, and should it be regulated in any one country in the absence of cooperation by others?" In a later section of this chapter, we examine some controversies affecting consensus at the international level with regard to regulatory schemes and practices.
Despite some of the controversies and challenges that arise in schemes for regulating cyberspace, Weckert and Al-Saggaf (2008) note that we should not presume against Internet regulation. In fact, they believe that a "strong moral case can be made for regulating the content of the Internet." Before proceeding with specific issues affecting the regulation of cyberspace, it is useful to consider two additional questions:

What do we mean by *cyberspace*?

What do we mean by *regulation*, particularly as it applies to cyberspace?

6.1.1 The ontology of Cyberspace: Is the Internet a Medium or a Place?

Some believe that the Internet is best understood as a new kind of medium, significantly different from earlier media, such as the telephone or television. Whereas the telephone is a "one-to-one medium," and television is a "one-to-many medium," Mike Goodwin (1995, 2003) describes the Internet as a "many-to-many medium." He also notes that one does not need to be wealthy to have access to this medium; nor does one need to win the approval of an editor or a publisher to speak his or her mind there. But is the Internet a medium, or can it be better understood as a public space?

Jean Camp and Y. T. Chien (2000) differentiate four types of media: *publisher*, *broadcast*, *distributor*, and *common carrier*. An example of a publisher is a newspaper or a magazine, and broadcast media include television and radio. Telephone companies and cable companies are instances of common carriers, conduits for the distribution of information. Camp and Chien argue that none of the media models are appropriate for understanding the Internet. Instead, they believe that a spatial modelone in which cyberspace is viewed as a public space with certain digital characteristicsis more plausible.

But can we model the Internet accurately as a public space, as Camp and Chien suggest? Or is it better understood as a new kind of medium, as Goodwin and others have argued? We are making more than a mere semantic distinction, because, as Camp and Chien point out, the model we use can influence our decisions about public policies on the Internet. If the Internet is viewed as a public space, for example, then there are good legal and moral reasons for ensuring that everyone has access to it. The ontology of cyberspace will ultimately determine whether and how we should (or perhaps should not) regulate it.

Consider the rules used to regulate the distribution and sale of adult magazines and videos in physical space. Bookstores and video rental stores are permitted to carry and sell such merchandise, and because a store is a physical place, certain sections can be partitioned so that adults can visit them but individuals under a certain age cannot. The rules are drastically different, however, for broadcast media such as television, where the Federal Communications Commission (FCC) regulates which kinds of content can be broadcast over the airwaves. Movies that can be rented and sold only to adults in stores can also be deemed inappropriate (by the FCC) for general television viewers. So before we can successfully resolve questions about Internet regulation, we need to keep in mind that the model we use to understand cyberspace will also strongly influence which regulatory schemes are appropriate.

6.1.2 Two categories of Cyberspace regulation

To regulate means to monitor or control a product, process, or set of behaviors according to certain requirements, standards, or protocols. Sometimes regulatory discussions about cyberspace have centered on its *content*, for example, whether online pornography and hate speech should be censored. And sometimes the regulatory discussions have focused on which kinds of processes, that is, rules and policies, should be implemented and enforced in commercial transactions in cyberspace. Physical space is regulated in both ways.

First, we can ask how we can possibly regulate cyberspace, which is inherently decentralized. Cyberspace is not compartmentalized neatly into state jurisdictions that can

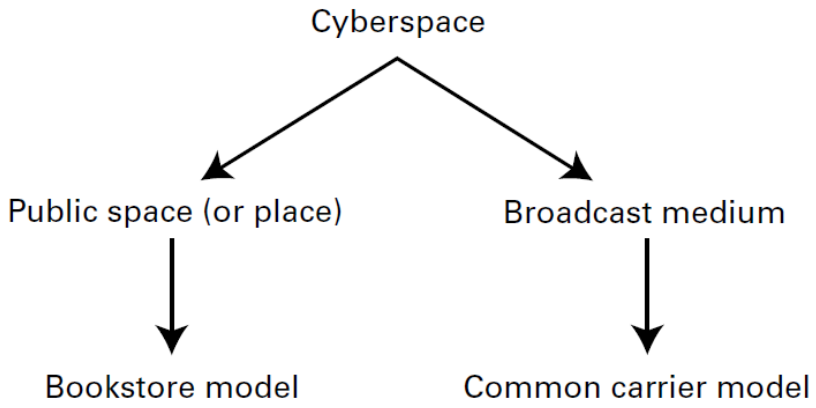


Figure 4: Ontology of cyberspace

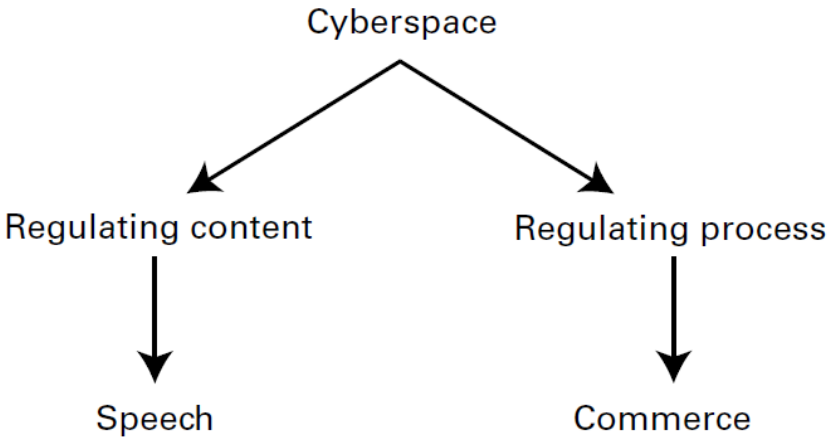


Figure 5: Two categories of cyberspace regulation

set up their own control boards. Does this mean that effective regulation of any type is impossible in cyberspace? Not according to Lawrence Lessig (2000) and Philip Agre (2005), who suggest that a decentralized cyberspace does not preclude Internet regulation from being carried out quite effectively. In describing the architecture of P2P (peer-to-peer) networks in cyberspace, Agre notes that decentralized institutions do not imply decentralized architectures, and vice versa. Lessig believes that in cyberspace, understanding architecture, or what he calls code, is the key to understanding how regulation works.

6.2 Four modes of regulation: the Lessig Model

Lessig describes four distinct but interdependent constraints, which he calls "modalities," for regulating behavior: *laws*, *social norms*, *market pressures*, and *architecture*. Before we apply each modality to cyberspace, consider how each can be applied in regulating behaviors in the physical world.

Cigarette smoking can be regulated through the passage and enforcement of explicit laws that make it illegal to smoke in public buildings. And we have specific laws that prohibit cigarette manufacturers from advertising on television or in magazines targeted at teenage audiences. Independent of explicit laws, however, social norms can also discourage cigarette smoking in public; for example, it is socially acceptable for homeowners to place Thank you for not smoking in our house signs on their front doors. And restaurant owners can, under social pressure from patrons, partition smoking and nonsmoking sections of their establishments even when there is no explicit law requiring them to do so. Market pressures can also affect smoking behavior. Cigarettes can be priced so that only the wealthiest people can afford to buy them. Finally, merchants can impose an architecture of control on cigarettes by using physical constraints. All cigarettes sold in grocery stores could be located behind locked doors, causing interruptions in check-out transactions. A cashier might have to temporarily suspend the transaction, locate the stores manager, and get the proper authorization and the key to open the locked doors to remove the cigarettes. Contrast this architecture with one in which cigarettes are available in vending machines easily accessible to everyone, including minors.

To apply Lessigs four-fold distinction to cyberspace, we replace architecture, which is in physical or geographic space, with *code*. Code, for Lessig, consists of programs, devices, and protocolsthat is, the sum total of the software and hardwarethat constitute cyberspace. Like physical architecture in geographic space, code sets the terms upon which one can enter or exit cyberspace. Also like architecture, code is not optional. Lessig notes that we do not choose to obey the structures that architecture establishes. Just as we are subject to architectures of physical space, so we are subject to code in cyberspace; a physical door can block you from entering a physical building, and a password requirement can prevent your entering a Web site. And code can be used to limit access to Web sites by requiring that users accept cookies (see Chapter 5) if they wish to visit those sites. Lessig believes that code can either facilitate or deter access to, or transfer of, information in cyberspace.

In Chapter 1, we saw that James Moor (2007) described computer technology as logically malleable because, unlike most other technologies that are dedicated to performing specific tasks, computers can be instructed through software to perform an indefinite number of diverse functions. Lessig (2004) also recognizes that computer technology is not fixed, noting that different computer architectures create very different kinds of environments.

Lessig concludes that we have moved from an architecture of freedom to an architecture of control. He also concludes that in cyberspace, code is a more effective regulator than law. In fact, Lessig claims that in cyberspace, code is the law.

6.3 Digital Rights Management and the Privatisation of Information Policy

To understand the force of Lessigs claim that code is regulating cyberspace, consider the role that software code in the form of DRM technologies play in regulating digital media. DRM technologies allow content owners to regulate the flow of information included in digital media by blocking access to it via encryption mechanisms, and by enabling access to it through the use of passwords. The combination of DRM technology and copyright protection laws, such

as the Digital Millennium Copyright Act (DMCA), has made possible the regulation and enforcement of policies and laws in cyberspace to a degree that never existed in the physical realm. As we saw in Chapter 8, theDMCAprohibits the development and use of technologies designed to circumvent copyright management systems. As a result, theDMCAworks hand in hand withDRMtechnology to control the flow of information in digitized form; any programs designed to circumvent DRM controls are in violation of Section 1201 of the DMCA.

6.3.1 DRM Technology: Implications for Public Debate on Copyright Issues

Critics worry about the ways in which DRM technology can be used to enforce copyright law. Because software code in DRM systems is being developed and used with the express purpose of precluding the possibility of copyright infringement, Niva Elkin- Koren (2000) fears that the traditional mechanism for debating public policy may now be closed to us. She notes that if computer manufacturers can decide what the copyright rules should be, and if they are permitted to embed code in their products that enforces those rules, then there is no longer a need for, or even the possibility of, public policy debate about copyright issues.

In the past, when individuals duplicated proprietary information by using the latest available technologies, we were often forced to question the viability of existing copyright laws in light of those new technologies vis-a-vis principles such as fair use and first sale (described in Chapter 8). Elkin-Koren notes that we could then engage in meaningful public policy debates about whether traditional copyright laws should apply or whether some new laws are needed. Most importantly, we could challenge the viability and constitutionality of such laws through the judicial process.

Elkin-Koren worries that a framework for *balancing* the interests of individuals and the public, which in the past had been supported by spirited policy debates and judicial review, will no longer be possible in a world in which copyright policies are predetermined by code. As Richard Spinello (2003) notes, restrictions embedded into computer code end up having the force of law without the checks and balances provided by the legal system.

Pamela Samuelson (2003), who also has been critical of technologies that regulate through embedded code, believes thatDRMsystems may violate the fair-use provision of copyright law. She notes that DRM technology allows content owners to exercise far more control over uses of copyrighted works in digital media than what is provided by conventional copyright law. Frances Grodzinsky and Maria Bottis (2007) also argue that DRM threatens the fair-use provision of copyright law. They believe that because of the way DRM is designed to protect digital content, our conventional understanding of private use as fair use has changed.

Other critics worry about the ways DRM systems can be abused by content owners to control users computers and to spy on unsuspecting users. Because of these and related factors, some now believe that DRM technology has gone too far. Can users trust content owners, such as Sony BMG, who are easily able to spy on them and able to control aspects of their computers and electronic devices via the use of DRM technology? Are Sonys actions justified on grounds that companies need DRM systems to protect their intellectual property rights?

Another area of tension involving DRM and the music industry has to do with

interoperability across the devices on which music can be played. Interoperability enables users to download and play music on a variety of devices. However, it also challenges the notion that downloadable content can and should be restricted to proprietary devices controlled by the company that owns an online store, such as iPods in the iTunes store. Internationally, there have been some efforts to promote interoperability. For example, in 2006, Frances National Assembly passed a law that would force distributors of online music in France to remove DRM so that music can be played on any device. Some believe that this move could pave the way for other EU countries to follow (Hesseldahl 2006). However, many owners and distributors of music content believe that removing DRM to support interoperability could also result in opening the door to file sharing of copyrighted material without compensation for the content owners and distributors.
In 2007, EMI announced that it would sell its music without DRM on Apple Corporations iTunes music store. One tradeoff, however, was that non-DRM-formatted music would cost slightly more than DRM versions. Proponents of this change, including the late Steve Jobs (2007), believe that if DRM restrictions were lifted on music, there might be an influx of new stores and players. But the debate about DRM in the contexts of online music and interoperability continues.

6.3.2 Privatizing Information Policy: Implications for the Internet

We have seen thatDRMschemes tip the balance in favor of the copyright owner who can determine how and by whom his/her content may be used. For that reason, DRM has become an obstacle to fair use because it limits the users freedom by allowing private interests to define the parameters of the law. Elkin-Koren argues that because of the technological controls embedded in software code (such as inDRMsystems), our policies affecting information and digital media are becoming increasingly *privatized*. She also notes that this trend toward privatization has enabled software companies to design code that reflects their own interests and values, without having to worry about any adverse effects that code can have for the publics interests.
Jessica Litman (2002) is also concerned about efforts that have been made to privatize information policies in cyberspace via the use of technology and law. She describes how the Recording Industry of America (RIAA) tried to pressure computer manufacturers to embed code in their computer systems that would make it impossible to use personal computers to download MP3 files and to burn CDs. Litman also notes that, in the late 1990s, the recording industry sought legislation that would ban the manufacture of portable MP3 players on grounds that such devices could be used to play pirated music, even though the MP3 file format is perfectly legal and even though many MP3 files do not contain copyrighted music.
Some critics worry about potential conflicts of interest that arise in the e-commerce sector in connection with the trend toward privatization. These critics note that lines have begun to blur between common carriers (such as telephone companies) and commercial content providers, which in the past were closely regulated and monitored by the FCC. For example, consider that the business merger involving AOL and the Time Warner Corporation in 2001 brought together a carrier and a content provider under the umbrella

of one major corporation. Mergers of this type have created conflicts of interest because the content provided by a company such as Time Warner could receive preferential consideration in offerings provided to AOL subscribers. We examine some aspects of this concern in detail in Section 9.9, where we analyze controversies surrounding "network neutrality".

6.4 The use and misuse of of (HTML) metatags and web hyperlinks

We have seen how some information policies, in conjunction with technologies such as DRM, increasingly privatize cyberspace. And we have seen how policies involving the assignment of Internet domain names can favorably affect the interests of some individuals and organizations in the e-commerce sector, at the expense of others. In this section, we consider some controversies surrounding the use (and abuse) of hypertext markup language (HTML) metatags in software code. Another code-related controversy that we examine is the use of deep linking, a form of hyperlinking, to access targeted sections of Web sites.

6.4.1 Issues surrounding the use/abuse of HTML metatags

A metatag is a string of text that is embedded inHTML code. To see which metatags have been included in a Web site, one can view the HTML source code used to construct the site, and most Web browsers enable users to do this. Metatags can be either keyword metatags or descriptive metatags. Keyword metatags, such as ¡football¿ and¡Aaron Rodgers¿ enable Web-site designers to identify terms that can be used by search engines. Descriptive metatags, on the contrary, enable the designer of a Web page to describe the page contents. For example, the description of aWebsite for AaronRodgers might read: "AaronRodgers ... quarterback for the Green Bay Packers ... received the NFLs Most Valuable Player award for the 20112012 season ... " The description typically appears as one or more sentence fragments, directly beneath the Web sites listing in an Internet search result.

Search engines examine keyword metatags to help determine how best to organize the listings ofWeb sites they return to queries, according to meaningful categories that a user might request.

Metatags hardly seem controversial; however, they can be used for deceptive purposes.

6.4.2 Hyperlinking and deep linking

Users can navigate the Web from one site to another via direct connections called hyperlinks. Clicking on a hyperlink takes the user directly to the target Web site. Without hyperlinks, users have to either use search engines to locate and access related Web sites before being able to link to themor enter by hand (i.e., key in) the complete URL of a site in order to access it.

Before the e-commerce era, the practice of including direct links to related Web pages had become the default mode of operation on the Web; Internet users gave little thought as

to whether they needed permission to include a hyperlink to a target Web site (or to any particular section of that targeted site). They did not consider, from a legal perspective, whether they had an explicit right to link directly to another persons Web site, or to any portion of it, without first acquiring the express consent of its owner.
Operators of some commercial Web sites have objected to visitors linking deep into their sites, thus bypassing the toplevel pages. They point out that online advertisers, who typically place advertisements on the top-level pages of Web sites, want their ads to be seen by all visitors to the sites they are sponsoring.
Also, counter mechanisms (which track both the number of users who visit a site over a certain period and information about the time of day most visitors connect to that site) have been included on a commercial Web sites top-level page, and this kind of information can be a key factor in determining whether advertisers will sponsor a particular site. Commercial Web-site owners, especially those who depend on advertisers, have been concerned about how users access their sites.
Those who operate noncommercial Web sites might also want to be able to exercise control over how visitors enter their sites, just as a homeowner may prefer that guests enter his house by way of the front door instead of the side or back door. We next consider two examples of deep linking: one in a commercial context, and the other in a personal Web site.
If a Web site is viewed as a form of (intellectual) property, then she may have a strong case. Consider that Maria, as a property owner, could determine how people enter her site in the same way that a home owner in physical space can require that visitors enter the house only through either the front door or a side door. If a Web site is considered private property, however, another controversial issue also arises: an unwelcome visitor to a Web site could be accused of trespassing. The notion of trespass in cyberspace is far from clear; however, some believe that the practice of sending unsolicited e-mail, which is now commonly referred to as spam, qualifies as a form of trespass in cyberspace.

6.5 Email spam

6.5.1 Defining Spam

While there is no universally agreed-upon definition of spam, it is typically viewed as e-mail that is unsolicited, commercial, and sent in bulk to multiple users. Is this definition adequate? Because spam is unsolicited, it is also nonconsensual. However, not all nonconsensual e-mail is spam. If you have an e-mail account, you have probably received unsolicited e-mail messages requesting information from you or informing you about an upcoming event; they may have been sent to you because you are a member of a particular social networking service (SNS) or because you have an e-mail address associated with an academic institution, government organization, and so forth. You may have considered some of these messages annoying, but are they necessarily spam?
Another feature of our working definition of spam is that it is commercial. However, some commercial e-mail you receive can be in the form of advertisements that you have authorized a commercial Web site to e-mail you. For example, you could have registered on an e-mail distribution list for a department store at which you frequently shop, requesting to be informed about upcoming sales and discount items. The e-mails you receive from this site,

while commercial or promotional in nature, would not qualify as spam.
Spam is distributed in bulk, but not all e-mails distributed in that form necessarily qualify as spam. For example, some messages sent in bulk form (i.e., to an e-mail list) might have been directed at people in the group who are known by the sender; there could be some personal or professional connection between the sender and receiver of the e-mail message. So, our initial working definition of spam as e-mail that is unsolicited, promotional, and sent in bulk to multiple users would not seem adequate.
Miller and Moor believe that much of the popular discussion about spam in terms of what they describe as unsolicited commercial bulk e-mail (UCBE) is both confused and degraded because it fails to distinguish between UCBE that is "deceptive" and "intended to harm" and UCBE that is not. They also believe that the problems affecting e-mail spam can be better analyzed by focusing on a series of distinct, but interrelated, criteria such as the

- content of the e-mail
- intent of the sender
- consequences of the receiver
- consent of the receiver
- relationship between the sender and the receiver
- accountability of the sender and the degree of deception
- number of identical e-mails sent.

Miller and Moor disagree with many critics of spam who tend to assume that all e-mail advertisements are deceptive. Alternatively, they believe that it is possible to distinguish between UCBE advertisements that (a) "misrepresent and are fraudulent" and (b) "present information in a favorable light." They refer to the former as F-UCBE and distinguish it from the nonfraudulent version they call NF-UCBE. They also believe that NF-UCBE requires a more complex ethical analysis than F-UCBE.

6.5.2 Why is Spam Morally Objectionable?

Richard Spinello (2006) believes that spam is morally objectionable for two reasons: one based on utilitarian grounds and the other on deontological considerations. In his view, spam not only has harmful consequences, but it also violates the individual autonomy of Internet users.
First, consider some of the harmful consequences of spame.g., its financial impacts, such as cost shifting and the consumption of valuable network resources. For example, spam consumes and strains valuable computing resources and thus contributes to the degradation of what Spinello describes as the "fragile ecology of the Internet." Miller and Moor describe these kinds of abuses of the Internet as one more instance of "spoiling of the commons."
Spinello argues that even if Internet resources were infinite and there were no negative utilitarian consequences, spam would still be morally objectionable because it does not respect individual users as persons. He believes that deontological arguments, such as

Kants (see Chapter 2), can be used to show why this so. Recall that Kant argues that a practice has moral worth only if it can be universalizable. And, in Kants system, a practice is universalizable only if it can coherently apply to all persons without exception. So, we need to ask: Could we universalize a coherent practice in which each e-mail user would allow spam to be sent and received by every other user? Could such a practice, if instituted, be logically coherent? On Kantian grounds, if spammers did not accept the principle that everyone should be able to send and receive spam, then they would be inconsistent. If spammers believed that only they should be permitted to send spam, then they would be making an exception for themselves. And if they granted themselves this exception, while relying on the good will of ordinary users not to engage in the practice of spamming others, then spammers would be treating ordinary users merely as a means to their ends. So, Spinello makes a plausible case for why spam can be considered morally objectionable on deontological as well as utilitarian grounds.

Miller and Moor believe that an adequate ethical analysis of spam also needs to take into consideration criteria such as accountability and deceptiongenerally, the more deceptive the content and the less accountable the sender, the more blameworthy the sender becomes. Employing their distinction between NF-UCBE and F-UCBE, they argue that fraudulent UCBE should always be condemned, whereas some cases of NFUCBE can be justifiable from a moral point of view. For example, they point out that a whistle-blower might send a message to a large commercial mailing list to alert recipients of an injustice or a danger. Here, the whistle-blower may have justifiable reasons for sending the e-mail broadly and for wishing to be anonymous. Miller and Moor believe that in this whistle-blowing scenario, the intent of the sender needs to be taken into consideration. So, there can be some cases where sending spam in the form of NF-UCBE would be justifiable.

Miller and Moor believe that an adequate ethical analysis of spam also needs to take into consideration criteria such as accountability and deceptiongenerally, the more deceptive the content and the less accountable the sender, the more blameworthy the sender becomes. Employing their distinction between NF-UCBE and F-UCBE, they argue that fraudulent UCBE should always be condemned, whereas some cases of NFUCBE can be justifiable from a moral point of view. For example, they point out that a whistle-blower might send a message to a large commercial mailing list to alert recipients of an injustice or a danger. Here, the whistle-blower may have justifiable reasons for sending the e-mail broadly and for wishing to be anonymous. Miller and Moor believe that in this whistle-blowing scenario, the intent of the sender needs to be taken into consideration. So, there can be some cases where sending spam in the form of NF-UCBE would be justifiable.

It is one thing to say that spam, at least in its F-UCBE form, is morally objectionable, but it is another to ask what can be done about it from a legal and a public policy perspective. Because spam is very similar to the junk mail that we receive via the postal delivery system, we might ask why the same laws that apply to physical junk mail do not also apply to electronic spam. Although there are similarities between the two forms of junk mail, there are also relevant differences; practical and financial constraints determine how much physical junk mail merchants can send, but the same kinds of constraints do not apply in the case of electronic spam.

Miller and Moor believe that e-mail spam is also analogous to unsolicited commercial phone calls. And they point out that the latter have been significantly reduced in the

United States through legislation, even though they have not been altogether eliminated. But they also note that because of the open nature of Internet architectures and protocols, spam has been far more resistant to the kinds of legislative and technological solutions used to discourage unsolicited commercial phone calls.