Collection of chapter summaries from *Ethics in Information Technology* (Reynolds, G. 6th edition, 2019)

Chapter 1 summary: An Overiview of Ethics

What is ethics?

•Ethics is a code of behavior that is defined by the group to which an individual belongs.

•Morals are the personal principles upon which an individual bases his or her decisions about what is right and what is wrong.

•A person who acts with integrity acts in accordance with a personal code of principles.

•Law is a system of rules that tells us what we can and cannot do. Laws are enforced by a set of institutions (the police, courts, and law-making bodies).

•A code of ethics states the principles and core values that are essential to one's work.

•Just because an activity is defined as legal does not mean that it is ethical.

What trends have increased the likelihood of an unethical behavior?

•Globalization has created a much more complex work environment, making it more difficult to apply principles and codes of ethics consistently.

•Organizations may be tempted to resort to unethical behavior to maintain profits in today's more challenging and uncertain economic climate.

•It is not unusual for powerful, highly successful individuals to fail to act in morally appropriate ways as such people are often aggressive in striving for what they want and are used to having privileged access to information, people, and other resources. Furthermore, their success often inflates their belief that they have the ability and the right to manipulate the outcome of any situation.

What is corporate social responsibility, and why is fostering good business ethics important?

•Corporate social responsibility is the concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers.

•Supply chain sustainability is a component of CSR that focuses on developing and maintaining a supply chain that meets the needs of the present without compromising the ability of future generations to meet their needs.

•Each organization must decide if CSR is a priority, and if so, what its specific CSR goals are.

•Organizations have five good reasons for pursuing CSR goals and promoting a work environment in which they encourage employees to act ethically: (1) to gain the goodwill of the community, (2) to create an organization that operates consistently, (3) to foster good business practices, (4) to protect the organization and its employees from legal action, and (5) to avoid unfavorable publicity.

What measures can organizations take to improve their business ethics?

•An organization can take several actions to improve its business ethics including: appointing a corporate ethics officer, requiring its board of directors to set and model high ethical standards, establish a corporate code of ethics, conduct social audits, require employees to take ethics training, include ethical criteria in employee appraisals, and create an ethical work environment.

How can you include ethical considerations in your decision making?

•Often, people employ a simple decision-making model that includes these steps: (1) define the problem, (2) identify alternatives, (3) choose an alternative, (4) implement the decision, and (5) monitor the results.

•You can incorporate ethical considerations into decision making by identifying and involving the stakeholders; weighing various laws, guidelines, and principles—including the organization's code of ethics—that may apply; and considering the impact of the decision on you, your organization, stakeholders, your customers and suppliers, and the environment.

What trends have increased the risk that information technology will be used in an unethical manner?

•The growth of the Internet and social networks; the ability to capture, store, and analyze vast amounts of personal data; and a greater reliance on information systems in all aspects of life have increased the risk that information technology will be used unethically.

•In the midst of the many IT breakthroughs in recent years, the importance of ethics and human values has been underemphasized—with a range of consequences.

Chapter 2 Summary: Ethics for IT Workers and IT Users

What relationships must an IT worker manage, and what key ethical issues can arise in each?

•An IT worker must maintain good working relationships with employers, clients, suppliers, other professionals, IT users, and society at large. Each relationship has its own set of ethical issues and potential problems.

•In relationships between IT workers and employers, important issues include setting and enforcing policies regarding the ethical use of IT, the potential for whistle-blowing, and the safeguarding of trade secrets.

•In relationships between IT workers and clients, key issues revolve around defining, sharing, and fulfilling each party's responsibilities for successfully completing an IT project. The IT worker must remain objective and guard against any sort of conflict of interest, fraud, misrepresentation, or breach of contract.

•A major goal for IT workers and suppliers is to develop good working relationships in which no action can be perceived as unethical.

•Bribery is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage.

- Internal control is the process established by an organization's board of directors, managers, and IT group to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations.

- Policies are the guidelines, standards, and laws by which the organization must abide. Policies drive processes and procedures. Processes are a collection of tasks designed to accomplish a stated objective. A procedure defines the exact instructions for completing each task in a process.

- A fundamental concept of good internal control is the careful separation of duties associated with any process that involves the handling of financial transactions so that different aspects of the process are handled by different people.

- The Foreign Corrupt Practices Act (FCPA) makes it a crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office. The act applies to any U.S. citizen or company and to any company with shares listed on any U.S. stock exchange.

- In relationships between IT workers and other professionals, the priority is to improve the profession through activities such as mentoring inexperienced colleagues, demonstrating professional loyalty, and avoiding résumé inflation and the inappropriate sharing of corporate information.

•In relationships between IT professionals and IT users, important issues include software piracy, inappropriate use of IT resources, and inappropriate sharing of information.

•When it comes to the relationship between IT workers and society at large, the main challenge for IT workers is to practice the profession in ways that cause no harm to society and provide significant benefits.

What can be done to encourage the professionalism of IT workers?

•A professional is one who possess the skill, good judgment, and work habits expected from a person who has the training and experience to do a job well.

•A professional is expected to contribute to society, to participate in a lifelong training program, to keep abreast of developments in the field, and to help develop other professionals.

•IT workers of all types can improve their profession's reputation for professionalism by (1) subscribing to a professional code of ethics, (2) joining and participating in professional organizations, (3) obtaining appropriate certifications, and (4) supporting government licensing where available.

•A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group.

•Codes of ethics usually have two main parts—the first outlines what the organization aspires to become and the second typically lists rules and principles that members are expected to live by. The codes also typically include a commitment to continuing education for those who practice the profession.

•Adherence to a code of ethics can produce many benefits for the individual, the profession, and society as a whole, including ethical decision making, high standards of practice and ethical behavior, trust and respect with the general public, and access to an evaluation benchmark that can be used for self-assessment.

•Several IT-related professional organizations have developed a code of ethics, including ACM, IEEE-CS, AITP, and SANS.

•Many people believe that the licensing and certification of IT workers would increase the reliability and effectiveness of information systems.

•Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Numerous companies and professional organization offer certification.

•Most states support the licensing of software engineers, and the state licensing boards have ultimate responsibility over specific requirements for licensing in their jurisdiction.

What ethical issues do IT users face, and what can be done to encourage their ethical behavior?

•IT users face several common ethical issues, including software piracy, inappropriate use of computing resources, and inappropriate sharing of information.

•Actions that can be taken to encourage the ethical behavior of IT users include establishing guidelines for the use of company hardware and software; defining an AUP for the use of IT resources; structuring information systems to protect data and information; installing and maintaining a corporate firewall; and ensuring compliance with laws, policies, and standards.

•The information security (infosec) group is responsible for managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and nondigital information.

•The audit committee of a board of directors and members of the internal audit team have a major role in ensuring that both the IT organization and IT users are in compliance with organizational guidelines and policies as well as various legal and regulatory practices.

Chapter 3 summary: Cyberattacks and Cybersecurity

Why are computer incidents so prevalent, and what are their effects?

•Increasing computing complexity, expanding and changing systems, an increase in the prevalence of BYOD policies, a growing reliance on software with known vulnerabilities, and the increasing sophistication of those who would do harm have caused a dramatic increase in the number, variety, and severity of security incidents.

•An exploit is an attack on an information system that takes advantage of a particular system vulnerability. Often this attack is due to poor system design or implementation.

•Many different types of people launch computer attacks, including the black hat hacker, cracker, malicious insider, industrial spy, cybercriminal, hacktivist, and cyberterrorist. Each type has a different motivation.

•A white hat hacker is someone who has been hired by an organization to test the security of its information systems allowing the organizations to improve its defenses.

•Ransomware, viruses, worms, Trojan horses, logic bombs, blended threats, spam, DDoS attacks, rootkits, advanced persistent threats, phishing, spear phishing, smishing, vishing, cyberespionage, and cyberterrorism are among the most common computer exploits.

•The DHS has the responsibility to provide for a “safer, more secure America, which is resilient against terrorism and other potential threats.” The agency's Office of Cybersecurity and Communications is responsible for enhancing the security, resilience, and reliability of U.S. cyber and communications infrastructure.

•The US-CERT is a partnership between DHS and the public and private sectors that was established to protect the nation's Internet infrastructure against cyberattacks by serving as a clearinghouse for information on new viruses, worms, and other computer security topics.

•Over the years, several laws have been enacted to prosecute those responsible for computer-related crime, including the Computer Fraud and Abuse Act, the Fraud and Related Activity in Connection with Access Devices Statute, the Stored Wire and Electronic Communications and Transactional Records Access Statutes, and the USA Patriot Act.

What can be done to implement a strong security program to prevent cyberattacks?

•The IT security practices of organizations worldwide must be focused on ensuring confidentiality, maintaining integrity, and guaranteeing the availability of their systems and data.

Confidentiality, integrity, and availability are referred to as the CIA security triad.

•An organization's security strategy must include security measures that are planned for, designed, implemented, tested, and maintained at the organization, network, application, and end-user levels.

•Every organization needs a risk-based strategy with an active governance process to minimize the potential impact of any security incident and to ensure business continuity in the event of a cyberattack. Key elements of such a strategy include a risk assessment to identify and prioritize the threats that the organization faces, a well-defined disaster recovery plan that ensures the availability of key data and information technology assets, definition of security policies needed to guide employees to follow recommended processes and practices to avoid security-related problems, periodic security audits to ensure that individuals are following established policies and to assess if the policies are still adequate even under changing conditions, compliance standards defined by external parties, and use of a security dashboard to help track the key performance indicators of their security strategy.

•The concept of reasonable assurance in connection with IT security recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.

•Authentication methods, a firewall, routers, encryption, proxy servers, VPN, and an IDS are key elements of the network security layer.

•Authentication methods, user roles and accounts, and data encryption are key elements of the application security layer.

•Security education, authentication methods, antivirus software, and data encryption are key elements of the end-user security layer.

What actions must be taken in the event of a successful security intrusion?

•No security system is perfect, so systems and procedures must be monitored to detect a possible intrusion. A response plan should be developed well in advance of any incident and be approved by both the organization's legal department and senior management. The response plan should address notification, evidence protection, activity log maintenance, containment, eradication, and follow-up.

•Organizations must implement fixes against well-known vulnerabilities and conduct periodic IT security audits.

•Many organizations outsource their network security operations to a MSSP, which is a company that monitors, manages, and maintains computer and network security for other organizations.

•Organizations must be knowledgeable of and have access to trained experts in computer forensics to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.

Chapter 4 summary: Privacy

What is the right of privacy, and what is the basis for protecting personal privacy under the law?

•The right of privacy is “the right to be left alone—the most comprehensive of rights, and the right most valued by a free people.”

•Information privacy is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one's personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use).

•The use of information technology in business requires balancing the needs of those who use the information that is collected against the rights and desires of the people whose information is being used. A combination of approaches—new laws, technical solutions, and privacy policies—is required to balance the scales.

•The Fourth Amendment reads, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The courts have ruled that without a reasonable expectation of privacy, there is no privacy right to protect.

•Today, in addition to protection from government intrusion, people want and need privacy protection from private industry. For many, the existing hodgepodge of privacy laws and practices fails to provide adequate protection and fuels a sense of distrust and skepticism, and concerns over identity theft.

What are some of the laws that provide protection for the privacy of personal data, and what are some of the associated ethical issues?

•Few laws provide privacy protection from private industry and there is no single, overarching national data privacy policy for the United States.

•The Fair Credit Reporting Act regulates operations of credit reporting bureaus.

•The Right to Financial Privacy Act protects the financial records of financial institution customers from unauthorized scrutiny by the federal government.

•The GLBA established mandatory guidelines for the collection and disclosure of personal financial information by financial institutions; requires financial institutions to document their data security plans; and encourages institutions to implement safeguards against pretexting.

•The Fair and Accurate Credit Transaction Act allows consumers to request and obtain a free credit report each year from each of the three consumer credit reporting agencies.

•The HIPAA defined numerous standards to improve the portability and continuity of health insurance coverage; reduce fraud, waste, and abuse in health insurance care and healthcare delivery; and simplify the administration of health insurance.

•The American Recovery and Reinvestment Act included strong privacy provisions for EHRs, including banning the sale of health information, promoting the use of audit trails and encryption, and providing rights of access for patients. It also mandated that each individual whose health information has been exposed be notified within 60 days after discovery of a data breach.

•The FERPA provides students and their parents with specific rights regarding the release of student records.

•The COPPA requires websites that cater to children to offer comprehensive privacy policies, notify parents or guardians about their data collection practices, and receive parental consent before collecting any personal information from children under the age of 13.

•Title III of the Omnibus Crime Control and Safe Streets Act (also known as the Wiretap Act) regulates the interception of wire (telephone) and oral communications.

•The FISA describes procedures for the electronic surveillance and collection of foreign intelligence information between foreign powers and agents of foreign powers.

•Executive Order 12333 identifies the various government intelligence-gathering agencies and defines what information can be collected, retained, and disseminated by the agencies. It allows for the tangential collection of U.S. citizen data—even when those citizens are not specifically targeted.

•The ECPA deals with the protection of communications while in transit from sender to receiver; the protection of communications held in electronic storage; and the prohibition of devices from recording dialing, routing, addressing, and signaling information without a search warrant.

•The CALEA requires the telecommunications industry to build tools into its products that federal investigators can use—after gaining a court order—to eavesdrop on conversations and intercept electronic communications.

•The USA PATRIOT Act modified 15 existing statutes and gave sweeping new powers both to domestic law enforcement and to international intelligence agencies, including increasing the ability of law enforcement agencies to eavesdrop on telephone communication, intercept email messages, and search medical, financial, and other records; the act also eased restrictions on foreign intelligence gathering in the United States.

•The Foreign Intelligence Surveillance Act Amendments Act of 2004 authorized intelligence gathering on individuals not affiliated with any known terrorist organization (so-called lone wolves).

•The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 granted the NSA expanded authority to collect, without court-approved warrants, international communications as they flow through the U.S. telecommunications equipment and facilities.

•The PATRIOT Sunsets Extension Act granted a four-year extension of provisions of the USA PATRIOT Act that allowed roving wiretaps and searches of business records. It also extended authorization intelligence gathering on "lone wolves."

•USA Freedom Act terminated the bulk collection of telephone metadata by the NSA instead requiring telecommunications carriers to hold the data and respond to NSA queries for data.

The act also restored authorization for roving wiretaps and the tracking of lone wolf terrorists.

•"Fair information practices" is a term for a set of guidelines that govern the collection and use of personal data. Various organizations as well as countries have developed their own set of such guidelines and call them by different names.

•The OECD for the Protection of Privacy and Transborder Data Flows of Personal Data created a set of fair information practices that are often held up as the model for organizations to adopt for the ethical treatment of consumer data.

•The European Union Data Protection Directive requires member countries to ensure that data transferred to non-EU countries is protected. It also bars the export of data to countries that do not have data privacy protection standards comparable to those of the EU. After the passage of this directive, the EU and the United States worked out an agreement that allowed U.S. companies that were certified as meeting certain "safe harbor" principles to process and store data of European consumers and companies.

•The European–United States Privacy Shield Data Transfer Program Guidelines is a stopgap measure that allows businesses to transfer personal data about European citizens to the United States. The guidelines were established after the European Court of Justice declared invalid the Safe Harbor agreement between the EU and the United States.

•The GDPR takes effect in May 2018 and addresses the export of personal data outside the EU enabling citizens to see and correct their personal data, standardizing data privacy regulations within the EU, and establishing substantial penalties for violation of its guidelines.

•The FOIA grants citizens the right to access certain information and records of the federal government upon request.

•The Privacy Act prohibits U.S. government agencies from concealing the existence of any personal data record-keeping system.

What are the various strategies for consumer profiling, and what are the associated ethical issues?

•Companies use many different methods to collect personal data about visitors to their websites, including depositing cookies on visitors' hard drives.

•Consumer data privacy has become a major marketing issue—companies that cannot protect or do not respect customer information have lost business and have become defendants in class actions stemming from privacy violations.

•A data breach is the unintended release of sensitive data or the access of sensitive data (e.g., credit card numbers, health insurance member ids, and Social Security numbers) by unauthorized individuals. The increasing number of data breaches is alarming, as is the lack of initiative by some companies in informing the people whose data are stolen. A number of states have passed data breach notifications laws that require companies to notify affected customers on a timely basis.

What is e-discovery, and how is it being used?

•Discovery is part of the pretrial phase of a lawsuit in which each party can obtain evidence from the other party by various means, including requests for the production of documents.

•E-discovery is the collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings.

•Predictive coding is a process that couples human intelligence with computer-driven concept searching in order to “train” document review software to recognize relevant documents within a document universe.

Why and how are employers increasingly using workplace monitoring?

•Many organizations have developed IT usage policies to protect against employee abuses that can reduce worker productivity and expose employers to harassment lawsuits.

•About 80 percent of U.S. firms record and review employee communications and activities on the job, including phone calls, email, web surfing, and computer files.

•The use of fitness trackers in the workplace has opened up potential new legal and ethical issues.

What are the capabilities of advanced surveillance technologies, and what ethical issues do they raise?

•Surveillance cameras are used in major cities around the world to deter crime and terrorist activities. Critics believe that such security is a violation of civil liberties.

•An EDR is a device that records vehicle and occupant data for a few seconds before, during, and after any vehicle crash that is severe enough to deploy the vehicle's air bags. The fact that most cars now come equipped with an EDR and that the data from this device may be used as evidence in a court of law is not broadly known by the public.

•Stalking apps can be downloaded onto a person's cell phone, making it possible to perform location tracking, record calls and conversations, view every text and photograph sent or received, and record the URLs of any website visited on that phone.

Chapter 5: Freedom of Expression

What is the basis for the protection of freedom of expression in the United States, and what types of expressions are not protected under the law?

•The First Amendment protects Americans' rights to freedom of religion, freedom of expression, and freedom to assemble peaceably. The Supreme Court has ruled that the First Amendment also protects the right to speak anonymously.

•Obscene speech, defamation, incitement of panic, incitement to crime, "fighting words," and sedition are not protected by the First Amendment and may be forbidden by the government.

What are some key federal laws that affect online freedom of expression, and how do they impact organizations?

•Although there are clear and convincing arguments to support freedom of speech on the Internet, the issue is complicated by the ease with which children can use the Internet to gain access to material that many parents and others feel is inappropriate for children. The conundrum is that it is difficult to restrict children's Internet access without also restricting adults' access.

•The U.S. government has passed several laws to attempt to address this issue, including the Communications Decency Act

(CDA), which is aimed at protecting children from online pornography, and the Child Online Protection Act (COPA), which prohibits making harmful material available to minors via the Internet. Both laws were ultimately ruled largely unconstitutional. However, Section 230 of the CDA, which was not ruled unconstitutional, provides immunity from defamation charges to ISPs that publish user-generated content, as long as they do not also serve as a content provider.

•Software manufacturers have developed Internet filters, which are designed to block access to objectionable material through a combination of URL, keyword, and dynamic content filtering.

•The Children's Internet Protection Act (CIPA) requires federally financed schools and libraries to use filters to block computer access to any material considered harmful to minors. In United States v. American Library Association, Inc., the American Library Association challenged CIPA. Ultimately in that case, the Supreme Court made it clear that the constitutionality of government-mandated filtering schemes depends on adult patrons' ability to request and receive unrestricted access to protected speech.

•The Digital Millennium Copyright Act (DMCA) addresses a number of copyright-related issues, with Title II of the act providing limitations on the liability of an ISP for copyright infringement.

What important freedom of expression issues relate to the use of information technology?

•Internet censorship is the control or suppression of the publishing or accessing of information on the Internet. There are many forms of Internet censorship. Many countries practice some form of Internet censorship.

•A SLAPP (strategic lawsuit against public participation) is a lawsuit filed by corporations, government officials, and others against citizens and community groups who oppose them on matters of concern. Anti-SLAPP laws are designed to reduce frivolous SLAPPs. As of 2015, 28 states and the District of Columbia have put into effect anti-SLAPP legislation to protect people who are the target of a SLAPP.

•Anonymous expression is the expression of opinions by people who do not reveal their identity. The freedom to express an opinion without fear of reprisal is an important right of a democratic society. Anonymity is even more important in countries that don't allow free speech. Maintaining anonymity on the Internet is important to some computer users. Such users sometimes use an anonymous remailer service, which strips the originating header and/or IP address from the message and then forwards the message to its intended recipient.

•Doxing involves doing research on the Internet to obtain someone's private personal information (such as home address, email address, phone numbers, and place of employment) and even private electronic documents (such as photographs), and then posting that information online without permission.

- Many businesses monitor the web for the public expression of opinions that might hurt their reputations. They also try to guard against the public sharing of company confidential information.

- Organizations may file a John Doe lawsuit to enable them to gain subpoena power in an effort to learn the identity of anonymous Internet users who they believe have caused some form of harm to the organization through their postings.

- In the United States, speech that is merely annoying, critical, demeaning, or offensive enjoys protection under the First Amendment. Legal recourse is possible only when hate speech turns into clear threats and intimidation against specific citizens.

- Some ISPs and social networking sites have voluntarily agreed to prohibit their subscribers and members from sending hate messages using their services. Because such prohibitions can be included in the service contracts between a private ISP and its subscribers or a social networking site and it members—and do not involve the federal government—they do not violate subscribers' First Amendment rights.

- Many adults, including some free-speech advocates, believe there is nothing illegal or wrong about purchasing adult pornographic material made by and for consenting adults. However, organizations must be very careful when dealing with pornography in the workplace. As long as companies can show that they were taking reasonable steps to prevent pornography, they have a valid defense if they are subject to a sexual harassment lawsuit.

•Reasonable steps include establishing a computer usage policy that prohibits access to pornography sites, identifying those who violate the policy, and taking action against those users—regardless of how embarrassing it is for the users or how harmful it might be for the company.

•Sexting—sending sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone—is a fast-growing trend that can lead to many problems for both senders and receivers.

•The Controlling the Assault of Non Solicited Pornography and Marketing (CAN-SPAM) Act specifies requirements that commercial emailers must follow when sending out messages that advertise a commercial product or service. The CAN-SPAM Act is also sometimes used in the fight against the dissemination of pornography.

•The proliferation of online sources of information and opinion means that the Internet is full of “news” accounts that are, in fact, highly opinionated, fictionalized, or satirical accounts of current events presented in journalistic style.

Chapter 6 summary: Intellectual property

What does the term intellectual property encompass, and what measures can organizations take to protect their intellectual property?

•Intellectual property is a term used to describe works of the mind—such as art, books, films, formulas, inventions, music, and processes—that are distinct and owned or created by a single person or group.

•Copyrights, patents, trademarks, and trade secrets form a complex body of law relating to the ownership of intellectual property, which represents a large and valuable asset to most companies. If these assets are not protected, other companies can copy or steal them, resulting in significant loss of revenue and competitive advantage.

•A copyright is the exclusive right to distribute, display, perform, or reproduce an original work in copies; to prepare derivative works based on the work; to and grant these exclusive rights to others.

•Copyright infringement is a violation of the rights secured by the owner of a copyright. Infringement occurs when someone copies a substantial and material part of another’s copyrighted work without permission.

•Copyright law has proven to be extremely flexible in covering new technologies, including software, video games, multimedia works, and web pages. However, evaluating the originality of a work can be difficult and disagreements over whether or not a work is original sometimes lead to litigation.

•Copyrights provide less protection for software than patents; software that produces the same result in a slightly different way may not infringe a copyright if no copying occurred.

•The fair use doctrine established four factors for courts to consider when deciding whether a particular use of copyrighted property is fair and can be allowed without penalty: (1) the purpose and character of the use, (2) the nature of the copyrighted work, (3) the portion of the copyrighted work used, and (4) the effect of the use on the value of the copyrighted work.

•The use of copyright to protect computer software raises many complicated issues of interpretation of what constitutes infringement.

•The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008 increased trademark and copyright enforcement; it also substantially increased penalties for infringement.

•The original General Agreement on Tariffs and Trade (GATT), signed in 1993, created the World Trade Organization (WTO) in Geneva, Switzerland, to enforce compliance with the agreement. GATT includes a section covering copyrights called the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

•The WTO is a global organization that deals with rules of international trade based on WTO agreements that are negotiated and signed by representatives of the world's trading nations The goal of the WTO is to help producers of goods and services, exporters, and importers conduct their business.

•The World Intellectual Property Organization (WIPO) is an agency of the United Nations dedicated to "the use of intellectual property as a means to stimulate innovation and creativity."

•The Digital Millennium Copyright Act (DMCA), which was signed into law in 1998, implements two WIPO treaties in the United States. The DMCA also makes it illegal to circumvent a technical protection or develop and provide tools that allow others to access a technologically protected work. In addition, the DMCA limits the liability of Internet service providers for copyright infringement by their subscribers or customers.

•Some view the DMCA as a boon to the growth of the Internet and its use as a conduit for innovation and freedom of expression. Others believe that the DMCA has given excessive powers to copyright holders.

•A patent is a grant of property right issued by the U.S. Patent and Trademark Office (USPTO) to an inventor that permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators. A patent prevents copying as well as independent creation (which is allowable under copyright law).

•For an invention to be eligible for a patent, it must fall into one of three statutory classes of items that can be patented: (1) it must be useful, (2) it must be novel, and (3) it must not be obvious to a person having ordinary skill in the same field.

•A utility patent is "issued for the invention of a new and useful process, machine, manufacture, or composition of matter, or a new and useful improvement thereof." A design patent, which is "issued for a new, original, and ornamental design embodied in or applied to an article of manufacture," permits its owner to exclude others from making, using, or selling the design in question.

•Unlike copyright infringement, for which monetary penalties are limited to certain specified dollar amounts, if the court determines that a patent has been intentionally infringed, it can award up to triple the amount of the damages claimed by the patent holder.

•The Leahy-Smith America Invents Act changed the U.S. patent system from a "first-to-invent" to a "first-inventor-to file" system and expanded the definition of prior art, which is used to determine the novelty of an invention and whether it can be patented. The act made it more difficult to obtain a patent in the United States.

•The courts and the U.S. Patent and Trademark Office (USPTO) have changed their attitudes and opinions of the patenting of software over the years.

•To qualify as a trade secret, information must have economic value and must not be readily ascertainable. In addition, the trade secret’s owner must have taken steps to maintain its secrecy. Trade secret laws do not prevent someone from using the same idea if it was developed independently or from analyzing an end product to figure out the trade secret behind it.

•Trade secrets are protected by the Uniform Trade Secrets Act, the Economic Espionage Act, and the Defend Trade Secrets Act, which amended the Economic Espionage Act to create a federal civil remedy for trade secret misappropriation.

•Trade secret law has three key advantages over the use of patents and copyrights in protecting companies from losing control of their intellectual property: (1) There are no time limitations on the protection of trade secrets, unlike patents and copyrights; (2) there is no need to file any application or otherwise disclose a trade secret to outsiders to gain protection; and (3) there is no risk that a trade secret might be found invalid in court.

•Because organizations can risk losing trade secrets when key employees leave, they often try to prohibit employees from revealing secrets by adding nondisclosure clauses to employment contracts. Employers can also use noncompete agreements to protect intellectual property from being used by competitors when key employees leave. A noncompete agreement prohibits an employee from working for any competitors for a period of time, often one to two years.

What are some of the current issues associated with the protection of intellectual property?

•Plagiarism is the act of stealing someone's ideas or words and passing them off as one's own. Plagiarism detection systems enable people to check the originality of documents and manuscripts.

•Reverse engineering is the process of breaking something down in order to understand it, build a copy of it, or improve it. It was originally applied to computer hardware but is now commonly applied to software.

•In some situations, reverse engineering might be considered unethical because it enables access to information that another organization may have copyrighted or classified as a trade secret.

•Recent court rulings and software license agreements that forbid reverse engineering, as well as restrictions in the DMCA, have made reverse engineering a riskier proposition in the United States.

- Open source code is any program whose source code is made available for use or modification, as users or other developers see fit. The basic premise behind open source code is that when many programmers can read, redistribute, and modify it, the software improves. Open source code can be adapted to meet new needs, and bugs can be rapidly identified and fixed.

- Competitive intelligence is legally obtained information that is gathered to help a company gain an advantage over its rivals. It is not the same as industrial espionage, which is the use of illegal means to obtain business information that is not readily available to the general public. In the United States, industrial espionage is a serious crime that carries heavy penalties.

- Competitive intelligence analysts must take care to avoid unethical or illegal behavior, including lying, misrepresentation, theft, bribery, or eavesdropping with illegal devices.

- A trademark is a logo, package design, phrase, sound, or word that enables a consumer to differentiate one company’s products from another’s. Website owners who sell trademarked goods or services must take care to ensure they are not sued for trademark infringement.

- Cybersquatters register domain names for famous trademarks or company names to which they have no connection, with the hope that the trademark’s owner will eventually buy the domain name for a large sum of money.

•The main tactic organizations use to circumvent cybersquatting is to protect a trademark by registering numerous domain names and variations as soon as they know they want to develop a web presence.

Chapter 7 Summary: Ethical Decisions in Software Development

What is meant by software quality, why is it so important, and what potential ethical issues do software manufacturers face when making decisions that involve trade-offs between project schedules, project costs, and software quality?

•High-quality software systems are easy to learn and use. They perform quickly and efficiently to meet their users’ needs, operate safely and reliably, and have a high degree of availability that keeps unexpected downtime to a minimum.

•High-quality software has long been required to support the fields of air traffic control, nuclear power, automobile safety, health care, military and defense, and space exploration.

•Computers and software are integral parts of almost every business, and the demand for high-quality software is increasing. End users cannot afford system crashes, lost work, or lower productivity. Nor can they tolerate security holes through which intruders can spread viruses, steal data, or shut down websites.

•A software defect is any error that, if not removed, could cause a software system to fail to meet its users' needs.

•Software quality is the degree to which a software product meets the needs of its users. Quality management focuses on defining, measuring, and refining the quality of the development process and the products developed during its various stages.

•Software developers are under extreme pressure to reduce the time to market of their products. They are driven by the need to beat the competition in delivering new functionality to users, to begin generating revenue to recover the cost of development, and to show a profit for shareholders.

•The resources and time needed to ensure quality are often cut under the intense pressure to ship a new software product. When forced to choose between adding more user features and doing more testing, many software companies decide in favor of more features.

•A business information system is a set of interrelated components—including hardware, software, databases, networks, people, and procedures—that collects and processes data and disseminates the output.

•Software product liability claims are typically based on strict liability, negligence, breach of warranty, or misrepresentation—sometimes in combination. Strict liability means that the defendant is held responsible for injuring another person regardless of negligence or intent.

•A warranty assures buyers or lessees that a product meets certain standards of quality and may be either expressly stated or implied by law. If the product fails to meet the terms of its warranty, the buyer or lessee can sue for breach of warranty.

What are some effective strategies for developing quality systems?

•A software development methodology is a standard, proven work process that enables systems analysts, programmers, project managers, and others to make controlled and orderly progress in developing high-quality software. Software methodologies define the activities in the software development process as well as the individual and group responsibilities for accomplishing objectives, recommend specific techniques for accomplishing the objectives, and offer guidelines for managing the quality of the products during the various stages of the development cycle.

•The waterfall system development model is a sequential, multistage system development process in which development of the next stage of the system cannot begin until the results of the current stage are approved or modified as necessary.

•Under the agile development methodology, a system is developed in iterations (often called sprints), lasting from one to four weeks. Agile development, which accepts the fact that system requirements are evolving and cannot be fully understood or defined at the start of the project, concentrates on maximizing the team's ability to deliver quickly and respond to emerging requirements.

•Using an effective development methodology enables a manufacturer to produce high-quality software, forecast project-completion milestones, and reduce the overall cost to develop and support software. An effective development methodology can also help protect software manufacturers from legal liability for defective software in two ways: by reducing the number of software errors that could cause damage and by making negligence more difficult to prove.

•The cost to identify and remove a defect in the early stages of software development can be up to 100 times less than removing a defect in a piece of software that has been distributed to customers.

•Quality assurance (QA) refers to methods within the development process that are designed to guarantee reliable operation of a product. Ideally, these methods are applied at each stage of the development cycle.

•There are several tests employed in software development including black-box and white-box dynamic testing, static testing, unit testing, integration testing, system testing, and user acceptance testing.

•Capability Maturity Model Integration (CMMI) models are collections of best practices that help organizations improve their processes. A best practice is a method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark within a particular industry. CMMI-Development (CMMI-DEV)—is frequently used to assess and improve software development practices.

•CMMI defines five levels of software development maturity: initial, managed, defined, quantitatively managed, and optimizing. CMMI identifies the issues that are most critical to software quality and process improvement. Its use can improve an organization’s ability to predict and control quality, schedule, costs, and productivity when acquiring, building, or enhancing software systems. CMMI also helps software engineers analyze, predict, and control selected properties of software systems.

•A safety-critical system is one whose failure may cause human injury or death. In the development of safety-critical systems, a key assumption is that safety will not automatically result from following an organization’s standard software development methodology.

- Safety-critical software must go through a much more rigorous and time-consuming development and testing process than other kinds of software; the appointment of a project safety engineer and the use of a hazard log and risk analysis are common in the development of safety-critical software.

- Risk is the potential of gaining or losing something of value. Risk can be quantified by three elements: a risk event, the probability of the event happening, and the impact (positive or negative) on the business outcome if the risk does actually occur.

- The annualized rate of occurrence (ARO) is an estimate of the probability that an event will occur over the course of a year. The single loss expectancy (SLE) is the estimated loss that would be incurred if the event happens. The annualized loss expectancy (ALE) is the estimated loss from this risk over the course of a year.

- The following equation is used to calculate the annual loss expectancy: ARO × SLE = ALE.

- Risk management is the process of identifying, monitoring, and limiting risks to a level that an organization is willing to accept.

- Reliability is a measure of the rate of failure in a system that would render it unusable over its expected lifetime.

- The International Organization for Standardization (ISO) issued its 9000 series of business management standards in 1988.

These standards require organizations to develop formal quality management systems that focus on identifying and meeting the needs, desires, and expectations of their customers.

•The ISO 9001 family of standards serves as a guide to quality products, services, and management; it provides a set of standardized requirements for a quality management system. Many businesses and government agencies specify that a vendor must be ISO 9001 certified to win a contract from them.

•Failure mode and effects analysis (FMEA) is an important technique used to develop ISO 9001–compliant quality systems. FMEA is used to evaluate reliability and determine the effects of system and equipment failures.

Chapter 8 summary: The Impact of Information Technology on Society

What is the relationship between IT investment and productivity growth in the United States?

•The most widely used measurement of the material standard of living is gross domestic product (GDP) per capita.

•In the United States, as in most developed nations, the standard of living has been improving over time. However, its rate of change varies as a result of business cycles that affect prices, wages, employment levels, and the production of goods and services.

•Labor productivity is a measure of the economic performance that compares the amount of goods and services produced with the number of labor hours used in producing those goods and services.

•Most countries have been able to produce more goods and services over time—not through a proportional increase in labor but rather by making production more efficient. These gains in productivity have led to increases in the GDP-based standard of living because the average hour of labor produced more goods and services.

•Innovation is a key factor in productivity improvement, and IT has played an important role in enabling innovation. Organizations use IT, other new technology, and capital investment to implement innovations in products, processes, and services.

•It can be difficult to quantify the benefits of IT investments on worker productivity because there can be a considerable lag between the application of innovative IT solutions and the capture of significant productivity gains. In addition, many factors other than IT influence worker productivity rates.

How will artificial intelligence, machine learning, robotics, and natural language processing affect the future workforce?

•Advances in artificial intelligence, machine learning, robotics, and natural language processing are fundamentally changing the way work gets done and have the potential to affect the tasks, roles, and responsibilities of most workers.

•Almost every job has partial automation potential and research suggests that 45 percent of human work activities could be automated using existing technology.

•It is likely to take decades for automation to achieve anywhere near its full potential.

•Artificial intelligence systems can simulate human intelligence processes, including learning, reasoning, and self-correction.

•Machine learning, a type of artificial intelligence (AI), involves computer programs that can learn some task and improve their performance with experience.

•Robotics is a branch of engineering that involves the development and manufacture of mechanical or computer devices that can perform tasks that require a high degree of precision or that are tedious or hazardous for human beings.

•Natural language processing is an aspect of artificial intelligence that involves technology that allows computers to understand, analyze, manipulate, and/or generate "natural languages" such as English.

What impact has the application of IT had on health care?

•Healthcare costs in the United States are expected to increase an average of 5.6 percent per year from 2016 to 2025.

•Much of this increase is due to the continued aging of the population, government policy, and life style changes, and to a lesser extent the development and use of new medical technology.

•In order for the United States to rein in healthcare spending, patient awareness must be raised and technology costs must be managed more carefully.

•An electronic medical record (EMR) is a collection of health-related information on an individual that is created, managed, and consulted by authorized clinicians and staff within a single healthcare organization. The information in an EMR is not easily shared with others outside of the healthcare organization where the data originated.

•An electronic health record (EHR) is a comprehensive view of the patient's complete medical history designed to be shared with authorized providers and staff from more than one organization.

•Health information exchange (HIE) is the process of sharing patient-level electronic health information between different organizations. HIE can result in more cost-effective and higher-quality care.

•A personal health record (PHR) includes those portions of the EHR that an individual patient "owns" and controls such as personal identifiers, contact information, health provider information, problem list, medication history, allergies, immunizations, and lab and test results.

•Clinical decision support (CDS) is a process and a set of tools designed to enhance health-related decision making through the use of clinical knowledge and patient-specific information to improve healthcare delivery. Effective use of CDS systems increases the quality of patient care while at the same time cutting costs.

•A computerized provider order entry (CPOE) system enables physicians to place orders (for drugs, laboratory tests, radiology, physical therapy) electronically with the orders transmitted directly to the recipient. CPOE streamlines the ordering process.

•Telehealth employs modern telecommunications and information technologies to provide medical care to people who live or work far away from healthcare providers, provide professional and patient health related training, and support healthcare administration.

•Telemedicine is the component of telehealth that provides medical care to people at a location different from the healthcare providers. Telemedicine helps reduce the need for patients to travel for treatment and allows healthcare professionals to serve more patients in a broader geographic area.

•Store-and-forward telemedicine involves acquiring data, sound, images, and video from a patient and then transmitting everything to a medical specialist for later evaluation.

Chapter 9 summary: Social Media

How do individuals use social networks, and what are some practical business uses of social networking and other social media tools?

•Social media are web-based communication channels and tools that enable people to interact with each other by creating online communities where they can share information, ideas, messages, and other content, including images, audio, and video.

•A social networking platform creates an online community of Internet users that enables members to break down barriers created by time, distance, and cultural differences; such a site allows people to interact with others online by sharing opinions, insights, information, interests, and experiences.

•The number of Internet users worldwide is approaching 4 billion or roughly half the population.

- Many organizations employ social networking platforms to advertise, identify and access job candidates, improve customer service, and sell products and services.

- An increasing number of business-oriented social networking platforms are designed to encourage and support relationships with consumers, clients, potential employees, suppliers, and business partners around the world.

- Social media marketing involves the use of social networks to communicate and promote the benefits of products and services.

- Two significant advantages of social media marketing over traditional marketing are that marketers can create a conversation with viewers of their ads and that ads can be targeted to reach people with the desired demographic characteristics.

- Social media marketing involves the use of social networks to communicate and promote the benefits of products and services. The two primary objectives of social media marketers are raising brand awareness and driving traffic to a website to increase product sales.

- Organic media marketing employs tools provided by or tailored for a particular social media platform to build a social community and interact with it by sharing posts and responding to customer comments on the organization's blog and social media accounts.

•Paid media marketing involves paying a third party to broadcast an organization's display ads or sponsored messages to social network users. Two common methods of charging for paid media are cost per thousand impressions and cost per click.

•Earned media refers to media exposure an organization gets through press and social media mentions, positive online ratings and reviews, tweets and retweets, reposts (or “shares”), recommendations, and so on. Earned social media traffic enables an organization to reach more people without any additional cost.

•Viral marketing is an approach to social media marketing that encourages individuals to pass along a marketing message to others, thus creating the potential for exponential growth in the message's exposure and influence.

•Some 60 percent of employers used social media to research job candidates with half of those finding information that gave a negative impression of the candidate.

•Employers can legally reject a job applicant based on the contents of the individual's social networking profile as long as the company is not violating federal or state discrimination laws.

•Job seeking candidates should review their presence on social media and remove photos and postings that portray them in a potentially negative light. Many jobseekers delete their social media accounts altogether.

•Increasingly, consumers are using social networks to share their experiences, both good and bad, with others. Because of this, many organizations actively monitor social media networks as a means of improving customer service, retaining customers, and increasing sales.

•A social shopping platform brings shoppers and sellers together in a social networking environment in which members share information and make recommendations while shopping online.

What are some of the key ethical issues associated with the use of social networks and other social media?

•Cyberabuse is any form of mistreatment or lack of care, both physical and mental, based on the use of an electronic communications device that causes harm and distress to others.

•Nearly three-quarters of U.S. Internet users have witnessed online harassment or abuse and almost half have personally experienced it.

•Cyberharassment is a form of cyberabuse in which the abusive behavior, which involves the use of an electronic communications device, is degrading, humiliating, hurtful, insulting, intimidating, malicious, or otherwise offensive to an individual or group of individuals causing substantial emotional distress.

•Cyberstalking is also a form of cyberabuse that consists of a long-term pattern of unwanted persistent pursuit and intrusive behavior (involving the use of an electronic communications device) that is directed by one person against another that causes fear and distress in the victim.

•The National Center for Victims of Crime offers tips on how to combat cyberstalking.

•The 1994 Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act set requirements for sex offender registration and notification in the United States. It also that states create websites that provide information on sex offenders within the state.

•The Sex Offender Registration and Notification Provisions (SORNA) of the Adam Walsh Child Protection and Safety Act of 2006 set national standards that govern which sex offenders must register and what data must be captured.

•Most social networking platforms have terms of use agreements, a privacy policy, or a content code of conduct that summarizes key legal aspects regarding use of the platform. Typically, the terms state that the platform has the right to delete material and terminate user accounts that violate its policies. These policies can be difficult to enforce.

•Inappropriate material posted online includes nonconsensual posts that include intimate photos or videos of people without their permission; such posts are often referred to as “revenge porn.” This type of content is often uploaded by ex-partners with an intention to shame, embarrass, and/or harass their former partner.

•The First Amendment of the U.S. Constitution protects the right of freedom of expression from government interference, however, it does not prohibit free speech interference by private employers.

•Organizations should put in place a social media policy to avoid legal issues and set clear guidelines and expectations for employees.

•The increased risk of accidents associated with social media interaction while driving, the tendency of many social media users to become narcissist in their postings, and the ability to perform self-image manipulation are additional social media issues.

<u>Chapter 10 summary: Ethics of IT Organizations</u>

What key legal and ethical issues are associated with the use of contingent workers, H-1B visa holders, and offshore outsourcing companies?

•Contingent work is a job situation in which an individual does not have an explicit or implicit contract for long-term employment.

•Organizations can obtain contingent workers through temporary staffing firms, employee leasing organizations, and professional employment organizations.

•Temporary staffing firms recruit, train, and test job seekers in a wide range of job categories and skill levels, and then assign them to clients as needed.

•In employee leasing, the subscribing firm transfers all or part of its workforce to the leasing firm, which handles all human-resource-related activities and costs such as payroll, training, and the administration of employee benefits. The subscribing firm leases these workers, but they remain employees of the leasing firm.

•A coemployment relationship is one in which two employers have actual or potential legal rights and duties with respect to the same employee or group of employees.

•A PEO is a business entity that hires the employees of its clients and then assumes all responsibility for all human resource management functions, including administration of benefits. The client company remains responsible for directing and controlling the daily activities of the employees. The client maintains a long-term investment and commitment to the employees, but uses the PEO as a means to outsource the human resource activities.

•The gig economy refers to a work environment in which temporary positions are common and organizations contract with independent workers for short-term engagements.

•An independent contractor is an individual who provides services to another individual or organization according to terms defined in a written contract or within a verbal agreement.

•Organizations that use contingent workers must be extremely careful how they pay and treat these workers, or run the risk of getting dragged into a class action lawsuit over mis-classification of workers.

•When a firm employs a contingent worker, it does not usually have to provide benefits, can easily adjust the number of workers to meet its business needs, and does not incur training costs.

•Contingent workers may have a low level of commitment to the company and its projects. The skills and knowledge a contingent worker gains while working for a particular are lost when the worker departs at a project's completion.

•An H-1B is a temporary work visa granted by the U.S. Citizenship and Immigration Services (USCIS) for people who work in specialty occupations—jobs that require at least a four-year bachelor's degree in a specific field, or equivalent experience.

•Employers hire H-1B workers to meet critical business needs or to obtain essential technical skills or knowledge that cannot be readily found in the United States. H-1B workers may also be used when there are temporary shortages of needed skills.

•Congress sets an annual cap on the number of H-1B visas to be granted—although the number of visas issued often varies greatly from this cap due to various exceptions.

•Companies applying for H-1B visas must offer a wage that is at least 95 percent of the average salary for the occupation. Because wages in the IT field vary substantially, unethical companies can get around the average salary requirement.

•Companies that employ H-1B workers are required to declare that they will not displace American workers; however, they are exempt from that requirement if 15 percent of more of their workers are on H-1B visas and the H-1B workers are paid at least $60,000 a year.

•Many U.S. companies complain they have trouble finding enough qualified workers and urge that the cap on visas be raised. Unemployed and displaced IT workers challenge whether the United States needs to continue importing tens of thousands of H-1B workers each year.

- The number of degrees awarded in the field of computer and information sciences at post-secondary institutions in the United States reached 130,000 in 2015. The Bureau of Labor Statistics has projected an increase of 53,000 new U.S. tech jobs per year from 2014 to 2024.
- Opinions vary as to whether or not the hiring of H-1B workers affects job opportunities and wages.
- Outsourcing is a long-term business arrangement in which a company contracts for services with an outside organization that has expertise in providing a specific function.
- Offshore outsourcing is a form of outsourcing in which the services are provided by an organization whose employees are in a foreign country.
- Outsourcing and offshore outsourcing are used to meet staffing needs while potentially reducing costs and speeding up project schedules.
- Many of the same ethical issues that arise when considering whether to hire H-1B and contingent workers apply to outsourcing and offshore outsourcing.
- Successful offshoring projects require day-to-day interaction between software development and business teams, so it is essential for the hiring company to take a hands-on approach to project management.

What is whistle-blowing, and what ethical issues are associated with it?

•Whistle-blowing is an effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by a company or some other organization.

•Whistle-blower protection laws allow employees to alert the proper authorities to employer actions that are unethical, illegal, or unsafe, or that violate specific public policies. Unfortunately, no comprehensive federal law protects all whistle-blowers from retaliatory acts.

•A potential whistle-blower must consider many ethical implications prior to going public with his or her allegations, including whether the high price of whistle-blowing is worth it; whether all other means of dealing with the problem have been exhausted; whether whistle-blowing violates the obligation of loyalty that the employee owes to his or her employer; and whether public exposure of the problem will actually correct its underlying cause and protect others from harm.

•An effective whistle-blowing process includes the following steps: (1) assess the seriousness of the situation, (2) begin documentation, (3) attempt to address the situation internally, (4) consider escalating the situation within the company, (5) assess the implications of becoming a whistle-blower, (6) use experienced resources to develop an action plan, (7) execute the action plan, and (8) live with the consequences.

What is green computing, and what are organizations doing to support this initiative?

•Green computing is concerned with the efficient and environmentally responsible design, manufacture, operation, and disposal of IT-related products.

•Green computing has three goals: (1) reduce the use of hazardous material, (2) allow companies to lower their power-related costs, and (3) enable the safe disposal or recycling of computers and computer-related equipment.

•Electronic Product Environmental Assessment Tool (EPEAT) is a system that enables purchasers to evaluate, compare, and select electronic products based on 51 environmental criteria.

•The European Union passed the Restriction of Hazardous Substances Directive to restrict the use of many hazardous materials in computer manufacturing, require manufacturers to use at least 65 percent reusable or recyclable components, implement a plan to manage products at the end of their life cycle in an environmentally safe manner, and reduce or eliminate toxic material in their packaging.