Unit 3: Privacy and Freedom of Expression

Syllabus:

Unit 3: Privacy and Freedom of Expression (10 Hrs.)

Privacy Protection and the Law - Information Privacy, Privacy Laws, Applications, and Court Rulings; Key Privacy and Anonymity Issues - Consumer Profiling, Electronic Discovery, Workplace Monitoring, Surveillance; First Amendment Rights; Freedom Expressions: Key Issues; Social Networking Ethical Issues

==========

Privacy Protection and the Law

The use of information technology in both government and 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.

Information about people is gathered, stored, analysed, and reported because organizations can use it to make better decisions as shown in figure below. Some of these decisions, including whether or not to hire a job candidate, approve a loan, or offer a scholarship, can profoundly affect people's lives. In addition, the global marketplace and intensified competition have increased the importance of knowing consumers' purchasing habits and financial condition. Companies use this information to target marketing efforts to consumers who are most likely to buy their products and services. Organizations also need basic information about customers to serve them better. It is hard to imagine an organization having productive relationships with its customers without having data about them. Thus, organizations want systems that collect and store key data from every interaction they have with a customer.

FIGURE Organizations gather a variety of data about people in order to make better decisions

However, many people object to the data collection policies of governments and businesses on the grounds that they strip individuals of the power to control their own personal information. For these people, the existing hodgepodge of privacy laws and practices fails to provide adequate protection; rather, it causes confusion that promotes distrust and skepticism, which are further fuelled by the disclosure of threats to privacy.

A combination of approaches like new laws, technical solutions, and privacy policies are required to balance the scales. Reasonable limits must be set on government and business access to personal information; new information and communication technologies must be designed to protect rather than diminish privacy; and appropriate corporate policies must be developed to set baseline standards for people's privacy. Education and communication are also essential.

This all will help you understand the right to privacy as well as the developments in information technology that could impact this right. It also addresses a number of ethical issues related to gathering data about people.

First, it is important to gain a historical perspective on the right to privacy. During the debates on the adoption of the U.S. Constitution, some of the drafters expressed concern that a powerful federal government would intrude on the privacy of individual citizens. After the Constitution went into effect in 1789, several amendments were proposed that would spell out additional rights of individuals. Ten of these proposed amendments were ultimately ratified and became known as the Bill of Rights. So, although the Constitution does not contain the word privacy, the U.S. Supreme Court has ruled that the concept of privacy is protected by the Bill of Rights. For example, the Supreme Court has stated that American citizens are protected by the Fourth Amendment when there is a "reasonable expectation of privacy."

The Fourth Amendment reads as follows:
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.

However, the courts have ruled that without a reasonable expectation of privacy, there is no privacy right.

Today, in addition to protection from government intrusion, people want and need privacy protection from private industry. Few laws provide such protection, and most people assume that they have greater privacy rights than the law actually provides. Some people believe that only those with something to hide should be concerned about the loss of privacy; however, others believe that everyone should be concerned. As the Privacy Protection Study Commission noted in 1977, when the computer age was still in its infancy: "The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small,

separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."

Many individuals are also concerned about the potential for a data breach in which personal data stored by an organization fall into the hands of criminals.

Table below shows about the system that gather data about individuals.

TABLE Systems that gather data about individuals

System/ program	Used by	How used
Automatic license plate readers (ALPRs)	Law enforcement agencies, including the U.S. Drug Enforcement Administration (DEA) and the U.S. Customs and Border Protection agency	ALPRs snap photos and document the location of vehicles; some systems can also photograph drivers and passengers. ALPRs are used to snag red-light runners and to identify motorists with outstanding arrest warrants, overdue parking tickets, and delinquent tax bills.
Backscatter imaging scanners	Law enforcement agencies, including the U.S. Customs and Border Protection agency, maritime police, general aviation security, and event security	Backscatter scanners can scan vehicles as well as individuals and crowds at public events to search for currency, drugs, and explosives.
Cookies	For-profit companies, nonprofit organizations, news and social media sites, and most other types of websites	Cookies capture your browsing history for website customization and personalization purposes and for targeted marketing purposes.
Drones	Law enforcement agencies, including the U.S. Customs and Border Protection agency	Drones are unmanned aerial vehicles used to support operations that require aerial surveillance.
Facebook tagging system	Facebook users	Facebook tags identify and reference people in photos and videos posted on Facebook by its more than 1 billion users.
Google location services	Smartphone and other mobile device users	Google's location services store a history of location data from all devices where a user is logged into a Google account.
MYSTIC	National Security Agency (NSA)	MYSTIC is used by the NSA to intercept and record all telephone conversations in certain countries, including Afghanistan, the Bahamas, Mexico, Kenya, and the Philippines. Because there is no practical way to exclude them, the conversations captured by MYSTIC include those of Americans who make calls to or from the targeted countries.[4,5]

TABLE Systems that gather data about individuals

System/ program	Used by	How used
PRISM	NSA	PRISM is an NSA surveillance program that collects Internet data, such as search histories; photos sent and received; and the contents of email, file transfers, and voice and video chats. PRISM also gathers data related to telephone calls, including the numbers of both parties on a call and the location, date, time, and duration of the call.
Secure Flight Program	Transportation Security Agency (TSA)	Secure Flight is an airline passenger prescreening program that checks travelers' personal information against the TSA's passenger watch list.
Smart TVs	Some TV manufacturers	Some smart TVs can capture personal conversations along with voice commands used to control the TV via their voice recognition system.
Stingray	Law enforcement agencies	Stingray is a type of hardware device used to impersonate a cell tower, forcing all mobile phones within range to connect to it. The device can then capture information that can be used to identify and locate users and the phone numbers they call or text.
Surveillance cameras	Law enforcement agencies	Cameras are used for intelligence gathering, the prevention of crime, and the protection of individuals or an object, and to support the investigation of a crime.

Information Privacy

A broad definition of 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." Another concept of privacy that is particularly useful in discussing the impact of IT on privacy is the term information privacy, first coined by Roger Clarke, director of the Australian Privacy Foundation.

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 their use).

Privacy Laws, Applications, and Court Rulings

This all outlines a number of legislative acts that affect a person's privacy. Note that most of these actions address invasion of privacy by the government. Legislation that protects people from data privacy abuses by corporations is almost non-existent.

Although a number of independent laws and acts have been implemented over time, no single, overarching national data privacy policy has been developed in the United States. Nor is there an established advisory agency that recommends acceptable privacy practices to businesses. Instead, there are laws that address potential abuses by the government, with little or no restrictions for private industry. As a result, existing legislation is sometimes inconsistent or even conflicting.

The discussion is divided into the following topics:

1. financial data
2. health information
3. children's personal data
4. electronic surveillance
5. fair information practices and
6. access to government records.

Financial Data

Individuals must reveal much of their personal financial data in order to take advantage of the wide range of financial products and services available, including credit cards, checking and savings accounts, loans, payroll direct deposit, and brokerage accounts. To access many of these financial products and services, individuals must use a personal logon name, password, account number, or PIN. The inadvertent loss or disclosure of these personal financial data carries a high risk of loss of privacy and potential financial loss. Individuals should be concerned about how these personal data are protected by businesses and other organizations and whether or not they are shared with other people or companies.

- **Fair Credit Reporting Act (1970)**

The Fair Credit Reporting Act, regulates the operations of credit reporting bureaus, including how they collect, store, and use credit information. The act, enforced by the U.S. Federal Trade Commission, is designed to ensure the accuracy, fairness, and privacy of information gathered by the credit reporting companies and to provide guidelines for organizations whose systems that gather and sell information about people.

The act outlines who may access your credit information, how you can find out what is in your file, how to dispute inaccurate data, and how long data are retained. It also prohibits a credit reporting bureau from giving out information about you to your employer or potential employer without your written consent.

- **Right to Financial Privacy Act (1978)**

The Right to Financial Privacy Act, protects the records of financial institution customers from unauthorized scrutiny by the federal government. Prior to the passage of this act, financial institution customers were not informed if their personal records were being turned over for review by a government authority, nor could customers challenge government access to their records. Under this act, a customer must receive written notice that a federal agency intends to obtain his or her financial records, along with an explanation of the purpose for which the records are sought. The customer must also be given written procedures to follow if he or she does not wish the records to be made available. In addition, to gain access to a customer's financial records, the government must obtain one of the following:

- an authorization signed by the customer that identifies the records, the reasons the records are requested, and the customer's rights under the act;
- an appropriate administrative or judicial subpoena or summons;
- a qualified search warrant or a formal written request by a government agency (can be used only if no administrative summons or subpoena authority is available).

- **Gramm-Leach-Bliley Act (1999)**

The Gramm-Leach-Bliley Act (GLB Act or GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways financial institutions deal with the private information of individuals.

The Act consists of three sections:

- **The Financial Privacy Rule,** which regulates the collection and disclosure of private financial information;
- **The Safeguards Rule,** which stipulates that financial institutions must implement security programs to protect such information; and
- **The Pretexting provisions,** which prohibit the practice of pretexting or accessing private information using false pretenses. The Act also requires financial institutions to give customers written privacy policy notices that explain their information-sharing practices.

The purpose of the GLB Act is to ensure that financial institutions and their affiliates safeguard the confidentiality of personally identifiable information (PII) gathered from customer records in paper, electronic or other forms. The law requires affected companies to comply with strict guidelines that govern data security.

According to the law, financial institutions have an obligation to respect their customers' privacy and securely protect their sensitive personal information against unauthorized access.

GLBA compliance requires that companies develop privacy practices and policies that detail how they collect, sell, share and otherwise reuse consumer information. Consumers also must be given the option to decide which information, if any, a company is permitted to disclose or retain for future use.

Fair and Accurate Credit Transactions Act (2003)

The Fair and Accurate Credit Transactions Act was passed in 2003 as an amendment to the Fair Credit Reporting Act, and it allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies.

The act also helped establish the National Fraud Alert system to help prevent identity theft. Under this system, consumers who suspect that they have been or may become a victim of identity theft can place an alert on their credit files. The alert places potential creditors on notice that they must proceed with caution when granting credit.

Health Information

The use of electronic medical records and the subsequent interlinking and transferring of this electronic information among different organizations has become widespread. Individuals are rightly concerned about the erosion of privacy of data concerning their health.

They fear intrusions into their health data by employers, schools, insurance firms, law enforcement agencies, and even marketing firms looking to promote their products and services. The primary law addressing these issues is the Health Insurance Portability and Accountability Act (HIPAA).

- **Health Insurance Portability and Accountability Act (1996)**

The Health Insurance Portability and Accountability Act (HIPAA) was designed to improve the portability and continuity of health insurance coverage; to reduce fraud, waste, and abuse in health insurance and healthcare delivery; and to simplify the administration of health insurance.

To these ends, HIPAA requires healthcare organizations to employ standardized electronic transactions, codes, and identifiers to enable them to fully digitize medical records, thus making it possible to exchange medical data over the Internet.

Under the HIPAA provisions, healthcare providers must obtain written consent from patients prior to disclosing any information from their medical records. Thus, patients need to sign a HIPAA disclosure form each time they are treated at a hospital, and such a form must be kept on file with their primary care physician. In addition, healthcare providers are required to keep track of everyone who receives information from a patient's medical file.

HIPAA assigns responsibility to healthcare organizations, as the originators of individual medical data, for certifying that their business partners (billing agents, insurers, debt collectors, research firms, government agencies, and charitable organizations) also comply with HIPAA security and privacy rules.

- **The American Recovery and Reinvestment Act (2009)**

The American Recovery and Reinvestment Act is a wide-ranging act 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

Children's Personal Data

A recent survey revealed that teens spend more than nine hours per day on average watching television, playing video games, social networking, browsing websites, or doing other things on a computer, smartphone, or tablet. Tweens (children aged 8 to 12) spend about six hours on average consuming media. Many people feel that there is a need to protect children from being exposed to inappropriate material and online predators; becoming the target of harassment; divulging personal data; and becoming involved in gambling or other inappropriate behaviour.

To date, only a few laws have been implemented to protect children online, and most of these have been ruled unconstitutional under the First Amendment and its protection of freedom of expression.

- **Family Educational Rights and Privacy Act (1974)**

The Family Educational Rights and Privacy Act (FERPA) is a federal law that assigns certain rights to parents regarding their children's educational records. These rights transfer to the student once the student reaches the age of 18, or earlier, if he or she attends a school beyond the high school level. These rights include:

- the right to access educational records maintained by a school;
- the right to demand that educational records be disclosed only with student consent;
- the right to amend educational records; and
- the right to file complaints against a school for disclosing educational records in violation of FERPA.

- **Children's Online Privacy Protection Act (1998)**

According to the Children's Online Privacy Protection Act (COPPA) , any website that caters to children must offer comprehensive privacy policies, notify parents or guardians about its data collection practices, and receive parental consent before collecting any personal information from children under 13 years of age.

COPPA was implemented in 1998 in an attempt to give parents control over the collection, use, and disclosure of their children's personal information; it does not cover the dissemination of information to children. The law has had a major impact and has required many companies to spend hundreds of thousands of dollars to make their sites compliant; other companies eliminated preteens as a target audience.

Electronic Surveillance

It discusses about government surveillance, including various forms of electronic surveillance, as well as some of the laws governing those activities. In recent years, new laws addressing government surveillance have been added and old laws amended in reaction to the development of new communication technologies and a heightened awareness of potential terrorist threats.

Many of the resulting surveillance activities are viewed by some as an unconstitutional violation of the Fourth Amendment, which protects us from illegal searches and seizures. As a result, there are frequent court challenges to these government actions, as well as an ongoing public debate about whether such activities make us Americans safer or simply erode our rights to privacy. Some people also feel that our basic rights of freedom of expression and association are violated when the U.S. government conducts widespread electronic surveillance on U.S. citizens.

For instance, some people who belong to particular ethnic, religious, and social groups are concerned that private data collected by the government could at some point be used to identify and target them and their associates.

There is also concern that our past communications may be used in the future to implicate us in crimes that were once private and innocent acts. On the other hand, many Americans feel that the U.S. government is obligated to do all that it can do to provide for the security of its citizens, even it means violating some of the rights designed to protect our privacy. After all, they argue, if you are not doing anything "wrong," you should have no concerns.

Figure 4-2 provides a timeline for the enactment of some of the most significant laws and executive orders addressing issues of governmental surveillance.

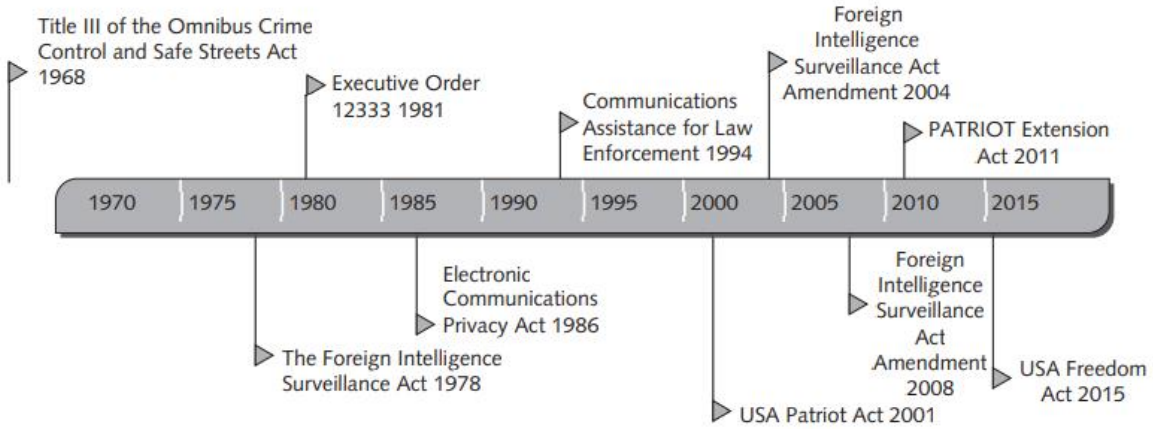

FIGURE 4-2 Various laws affecting electronic surveillance

Title III of the Omnibus Crime Control and Safe Streets Act (1968; amended 1986)

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. It allows state and federal law enforcement officials to use wiretapping and electronic eavesdropping, but only under strict limitations.

Under this act, a warrant must be obtained from a judge to conduct a wiretap. The judge may approve the warrant only if "there is probable cause that an individual is committing, has committed, or is about to commit a particular offense … [and that] normal investigative procedures have been tried and have failed or reasonably appear to be unlikely if tried or to be too dangerous."

The Foreign Intelligence Surveillance Act (1978)

The Foreign Intelligence Surveillance Act (FISA) describes procedures for the electronic surveillance and collection of foreign intelligence information in communications between foreign powers and the agents of foreign powers.

Foreign intelligence is information relating to the capabilities, intentions, or activities of foreign governments or agents of foreign governments or foreign organizations. The act allows surveillance, without court order, within the United States for up to a year unless the "surveillance will acquire the contents of any communication to which a U.S. person is a party."

If a U.S. citizen is involved, judicial authorization is required within 72 hours after surveillance begins. The act also specifies that the U.S. attorney general may request a specific communications common carrier (a company that provides communications transmission services to the public) to furnish information, facilities, or technical assistance to accomplish the electronic surveillance.

FISA requires the government to obtain an individualized court order before it can intentionally target a U.S. person anywhere in the world to collect the content of his/her communications. Under FISA, a U.S. person is defined as a U.S. citizen, permanent resident, or company.

Executive Order 12333 (1981)

An executive order is an official document used by the president of the United States to manage the operations of the federal government. Executive orders are subject to judicial review, and may be struck down if considered by the courts to be unsupported by statute or the Constitution. Many executive orders pertain to routine administrative matters and the internal operations of federal agencies.

However, some executive orders have a much more visible impact. For instance, in 1863, President Lincoln issued the Emancipation Proclamation, an executive order, to free all persons held as slaves in the United States, and in 1942, President Roosevelt issued an executive order to intern Japanese-Americans in prison camps.

Executive Order 12333, which was issued by President Reagan in 1981 and has been amended several times, identifies the various U.S. governmental intelligence-gathering agencies and defines what information can be collected, retained, and disseminated by these agencies.

Under Executive Order 12333, intelligence-gathering agencies are allowed to collect information—including message content—obtained in the course of a lawful foreign intelligence, counterintelligence, international drug, or international terrorism investigation, as well as incidentally obtained information that may indicate involvement in activities that may violate federal, state, local, or foreign laws. This tangential collection of U.S. citizen data—even when those citizens are not specifically targeted—is forbidden under FISA. Thus, there is an unresolved conflict between Executive Order 12333 and FISA.

TABLE 4-2 Intelligence-gathering units of the U.S. government defined in executive order 12333

Central Intelligence Agency	Defense Intelligence Agency	National Security Agency
National Reconnaissance Office	National Geospatial-Intelligence Agency	Intelligence and Counterintelligence elements of the Army, Navy, Air Force, Marine Corps, and Coast Guard
Federal Bureau of Investigation	Bureau of Intelligence and Research	Department of State
Office of Intelligence and Analysis	Department of Treasury	Office of National Security Intelligence
Drug Enforcement Administration	Department of Homeland Security	Office of Intelligence and Counterintelligence
Department of Energy	Office of the Director of National Intelligence	

Executive Order 12333 also approves the use of any intelligence collection techniques that are in accordance with procedures established by the head of the intelligence community and approved by the attorney general. There is limited congressional review and oversight of these procedures, and they have never been publicly debated or voted on by Congress.

Electronic Communications Privacy Act (1986)

The Electronic Communications Privacy Act (ECPA) deals with three main issues:

(1) the protection of communications while in transfer from sender to receiver;
(2) the protection of communications held in electronic storage; and
(3) the prohibition of devices from recording, dialling, routing, addressing, and signalling information without a search warrant.

Title I of ECPA extends the protections offered under the Wiretap Act to electronic communications, such as email, fax, and text messages sent over the Internet. The government is prohibited from intercepting such messages unless it obtains a court order based on probable cause (the same restriction that is in the Wiretap Act relating to telephone calls).

Title II of ECPA (also called the Stored Communications Act) prohibits unauthorized access to stored wire and electronic communications, such as the contents of email inboxes, text messages, message boards, and social networking sites.

However, the law only applies if the stored communications are not readily accessible to the general public.

Communications Assistance for Law Enforcement Act (1994)

The Communications Assistance for Law Enforcement Act (CALEA) was passed by Congress in 1994 and amended both the Wiretap Act and ECPA. CALEA was a hotly debated law because it required the telecommunications industry to build tools into its products that federal investigators could use—after obtaining a court order—to eavesdrop on conversations and intercept electronic communications.

Such a court order can only be obtained if it is shown that a crime is being committed, that communications about the crime will be intercepted, and that the equipment being tapped is being used by the suspect in connection with the crime.

A provision in the act covering radio-based data communication grew from a realization that the ECPA failed to cover emerging technologies, such as wireless modems, radio-based electronic mail, and cellular data networks. The ECPA statute outlawed the unauthorized interception of wire-based digital traffic on commercial networks, but the law's drafters did not foresee the growing interest in wireless data networks.

With CALEA, the Federal Communications Commission responded to appeals from the Department of Justice and other law enforcement officials by requiring providers of Internet phone services and broadband services to ensure that their equipment accommodated the use of law enforcement wiretaps. This equipment includes Voice over Internet Protocol (VoIP) technology, which shifts calls away from the traditional phone network of wires and switches to technology based on converting sounds into data and transmitting them over the Internet. The decision has

created a controversy among many who fear that opening VoIP to access by law enforcement agencies will create additional points of attack and security holes that hackers can exploit.

USA PATRIOT Act (2001)

The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) was passed just five weeks after the terrorist attacks of September 11, 2001.

It gave sweeping new powers to both domestic law enforcement and U.S. international intelligence agencies, including increasing the ability of law enforcement agencies to search telephone, email, medical, financial, and other records. It also eased restrictions on foreign intelligence gathering in the United States. Although the act was more than 340 pages long and quite complex (it changed more than 15 existing statutes), it was passed into law just five weeks after being introduced.

PATRIOT Sunsets Extension Act of 2011

The PATRIOT Sunsets Extension Act of 2011 granted a four-year extension of two key provisions in the USA PATRIOT Act that allowed roving wiretaps and searches of business records. This act also extended the 2004 FISA amendment that authorized intelligence gathering on "lone wolves." All three provisions are considered extremely useful by law enforcement officials but are opposed by some who say they can lead to privacy right abuses. These extensions were briefly allowed to expire in 2015 before being reinstated by the USA Freedom Act.

USA Freedom Act (2015)

The USA Freedom Act was passed following startling revelations by Edward Snowden (a former government contractor who copied and leaked classified information from the NSA in 2013 without authorization) of secret NSA surveillance programs.

Here is a partial list of those revelations:

- U.S. phone companies had been providing the NSA with all of their customers records, not just metadata (when each call was made and to what number).
- The NSA had been spying on over 120 world leaders, including German chancellor Angela Merkel, a U.S. ally.
- The NSA has developed a variety of tools to circumvent widely used Internet data encryption methods.
- An NSA team of expert hackers called the Tailored Access Operations hack into computers worldwide to infect them with malware.
- The FISA Court reprimanded the NSA for frequently providing misleading information about its surveillance practices.

Fair Information Practices

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 overall goal of such guidelines is to stop the unlawful storage of personal data, eliminate the storage of inaccurate personal data, and prevent the abuse or unauthorized disclosure of such data. For some organizations and some countries, a key issue is the flow of personal data across national boundaries (transborder data flow). Fair information practices are important because they form the underlying basis for many national laws addressing data privacy and data protection issues. Europe has been more active in this area than the United States and most of the national laws addressing data privacy originate in Europe

Organisation for Economic Co-operation and Development for the Protection of Privacy and Transborder Flows of Personal Data (1980)

The Organisation for Economic Co-operation and Development (OECD) is an international organization currently consisting of 35 member countries, including Australia, Canada, France, Germany, Italy, Japan, Mexico, New Zealand, Turkey, the United Kingdom, and the United States.

Its goals are to set policy and to come to agreement on topics for which multilateral consensus is necessary in order for individual countries to make progress in a global economy. Dialogue, consensus, and peer pressure are essential to make these policies and agreements stick.

European Union Data Protection Directive (1995)

The European Union Data Protection Directive requires any company doing business within the borders of the countries comprising the European Union (EU) to implement a set of privacy directives on the fair and appropriate use of information.

Basically, this 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.

The following list summarizes the basic tenets of the directive:

- Notice—An individual has the right to know if his or her personal data are being collected, and any data must be collected for clearly stated, legitimate purposes.
- Choice—An individual has the right to elect not to have his or her personal data collected.
- Use—An individual has the right to know how personal data will be used and the right to restrict their use.

- Security—Organizations must "implement appropriate technical and organizations measures" to protect personal data, and the individual has the right to know what these measures are.
- Correction—An individual has the right to challenge the accuracy of the data and to provide corrected data.
- Enforcement—An individual has the right to seek legal relief through appropriate channels to protect privacy rights.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR; officially known as Regulation EU 2016/679) is designed to strengthen data protection for individuals within the EU by addressing the export of personal data outside the EU, enabling citizens to see and correct their personal data, and ensure data protection consistency across the EU. Organizations anywhere in the world that collect, store, or transfer personal data of EU citizens must work to ensure that their systems and procedures are compliant with this strict new framework. Noncompliance can result in penalties for privacy violations amounting to as much as four percent of a company's annual global revenue.

When the GDPR takes effect in May 2018, it will repeal European Union Data Protection Directive (officially Directive 95/46/EC), the current data protection directive. That directive simply outlined recommendations and had no real enforcement requirements. This allowed the various EU countries to implement the recommendations as they saw fit, leading to significant differences from country to country. As a result, organizations operating in the EU have had to deal with a hodgepodge of data privacy laws governing the storing and processing of personal data. The GDPR regulation would simplify matters by enforcing a single set of rules for data protection across the EU. This will eliminate the need for costly administrative processes and save countries an estimated €2.3 billion (about $3.03 billion) per year. The GDPR would also likely replace the Privacy Shield Framework. The GDPR rules are more comprehensive than the Privacy Shield rules and include the right to be forgotten, which requires organizations to delete the personal data of European citizens upon request.

The United Kingdom's Tesco Bank was hit with a data breach in November 2016 that impacted some 40,000 customer accounts, with money taken from half of them.

Tesco Bank refunded £2.5 million ($3.2 million) to its current account customers following the attack. If the GDPR had been in effect at the time of the breach, Tesco Bank's parent company could have been facing a fine of nearly £2 billion ($2.5 billion).

Access to Government Records

The U.S. government has a great capacity to store data about each and every one of us and about the proceedings of its various agencies. The Freedom of Information Act (FOIA) enables the public to gain access to certain government records, and the Privacy Act prohibits the government from concealing the existence of any personal data record-keeping systems.

Freedom of Information Act (1966; amended 1974)

The Freedom of Information Act (FOIA) grants citizens the right to access certain information and records of federal, state, and local governments upon request. FOIA is a powerful tool that enables journalists and the public to acquire information that the government is reluctant to release. The well-defined FOIA procedures have been used to uncover previously unrevealed details about President Kennedy's assassination, determine when and how many times members of Congress or certain lobbyists have visited the White House, obtain budget and spending data about a government agency, and even request information on the "UFO incident" at Roswell in 1947 .

The FOIA is often used by whistle-blowers to obtain records that they would otherwise be unable to get. Citizens have also used FOIA to find out what information the government has about them. There are two basic requirements for filing a FOIA request:

(1) the request must not require wide-ranging, unreasonable, or burdensome searches for records and
(2) the request must be made according to agency procedural regulations published in the Federal Register.

A typical FOIA request includes the requester's statement: "pursuant to the Freedom of Information Act, I hereby request"; a reasonably described record; and a statement of willingness to pay for reasonable processing charges. (The fees can be substantial and include the cost to search for the documents, the cost to review documents to see if they should be disclosed, and the cost of duplication.) FOIA requests are sent to the FOIA officer for the responding agency.45 Agencies receiving a request must acknowledge that the request has been received and indicate when the request will be fulfilled. The act requires an initial response within 20 working days unless an unusual circumstance occurs. In reality, most requests take much longer. The courts have ruled that this is acceptable as long as the agency treats each request sequentially on a first-come, first-served basis. If a request filed under the FOIA is denied, the responding agency must provide the reasons for the denial along with the name and title of each denying officer. The agency must also notify the requester of his or her right to appeal the denial and provide the address to which an appeal should be sent. During 2015, the federal government processed a record high of 769,903 FOIA requests, with 37,860 requests (4.9 percent of the total filed) denied in full. An agency can deny a FOIA request based on the following nine document exemptions:

1. Information properly classified as secret in the interest of national security

2. Information related solely to internal personnel rules and practices of an agency
3. Information that is prohibited from disclosure based on other federal statutes
4. Trade secrets or privileged or confidential commercial or financial information
5. Privileged communications within or between agencies
6. A personnel, medical, or similar file the release of which would constitute a clearly unwarranted invasion of personal privacy .

Information compiled for law enforcement purposes, the release of which a. could reasonably be expected to interfere with law enforcement proceedings, b. would deprive a person of a right to a fair trial or an impartial adjudication, c. could reasonably be expected to constitute an unwarranted invasion of personal privacy, d. could reasonably be expected to disclose the identity of a confidential source, e. would disclose techniques, procedures, or guidelines for investigations or prosecutions, or f. could reasonably be expected to endanger an individual's life or physical safety.

Information that concerns the supervision of financial institutions 9. Documents containing exempt information about gas or oil wells The use of the FOIA to access information can lead to a dispute between those who feel it is important certain information be revealed and those who feel certain government data should not be made public, including, in some cases, those whose privacy is being impacted. Phil Eil has been attempting to write a book about the trial of Paul Volkman, a Chicago physician who was sentenced in 2012 to four consecutive life terms for illegally prescribing and distributing pain medications. Volkman's trial lasted eight weeks, and included 70 witnesses and over 220 exhibits.48 Following the trial, the DEA has prevented everyone from viewing the evidence from the trial. Eil was denied access to court documents by the U.S. district court clerk, appellate court clerk, the prosecutor, and the judge who presided over the case. Eil filed a FOIA request with the Department of Justice in 2012 but still was refused access. The denied request resulted in a lawsuit, which was filed in March 2015. Finally, in 2016, a U.S. district court judge ruled that Eil's request to view trial materials used to convict Volkman was legal and reasonable despite the DEA's insistence that the release would compromise the privacy of numerous people, including trial witnesses.49 The government can respond in various ways to FOIA requests other than by providing access to the full and unadulterated documents requested. For example, the ACLU filed a FOIA request for information regarding the Justice Department's policy on intercepting text messages on cellphones. In response, the ACLU received a 15-page response in which every single page was redacted from top to bottom.50 In 2014, journalist Victor Hugo Michel submitted a FOIA request for information about drug kingpin Joaquin "El Chapo" Guzman and was told that he would have to pay $1.46 million in fees to cover the cost of pulling information to meet his request.

Privacy Act (1974)

The Privacy Act establishes a code of fair information practices that sets rules for the collection, maintenance, use, and dissemination of personal data that is kept in systems of records by federal agencies. It also prohibits U.S. government agencies from concealing the existence of any personal data record-keeping system. Under this law, any agency that maintains such a system must publicly describe both the kinds of information in it and the manner in which the information will be used.

The law also outlines 12 requirements that each record-keeping agency must meet, including those that address issues such as openness, individual access, individual participation, collection limitation, use limitation, disclosure limitation, information management, and accountability. The purpose of the act is to provide safeguards for people against invasion of personal privacy by federal agencies.

The CIA and law enforcement agencies are excluded from this act; in addition, it does not cover the actions of private industry. Several individuals and organizations have attempted unsuccessfully to sue various federal agencies for what they perceive to be violations of the Privacy Act.

For instance, in 2004, miners sued the Department of Labor for disclosing their Social Security numbers in connection with the publication of their black lung compensation claims. The Supreme Court ruled in a case involving one of those miners that an individual can file suit against the government to recover financial damages when personal information is exposed only if an "actual damage" is proven, which it deemed the miner had not proved.

In 2011, the Department of Defense and Science Applications International Corporation (a provider of government services and information technology support) was sued under the Privacy Act after military health insurance data on 4.9 million service members and their families were stolen. In this case, a federal judge ruled that data loss alone, without evidence the information was misused, did not merit damages.53 In another case from 2012, the Supreme Court decided that a Federal Aviation Administration employee whose HIVpositive condition was disclosed could not claim financial damages based on mental or emotional distress caused by a federal agency's intentional or willful violation of the Privacy Act.

Key Privacy and Anonymity Issues

Privacy issues, includes

- Consumer profiling,
- Electronic discovery,
- Workplace monitoring, and
- Advanced surveillance technology.

Consumer Profiling

Companies openly collect personal information about users when they register at websites, complete surveys, fill out forms, follow them on social media, or enter contests online. Many companies also obtain personal information through the use of cookies— text files that can be downloaded to the hard drives of users who visit a website, so that the website is able to identify visitors on subsequent visits.

Companies also use tracking software to allow their websites to analyse browsing habits and deduce personal interests and preferences. After cookies have been stored on your computer, they make it possible for a website to tailor the ads and promotions presented to you. The marketer knows what ads have been viewed most recently and makes sure that they aren't shown again, unless the advertiser has decided to market using repetition. Some types of cookies can also track what other sites a user has visited, allowing marketers to use that data to make educated guesses about the kinds of ads that would be most interesting to the user.

Offline, marketing firms employ similarly controversial means to collect information about people and their buying habits. Each time a consumer uses a credit card, redeems frequent flyer points, fills out a warranty card, answers a phone survey, buys groceries using a store loyalty card, or registers a car with the DMV (Department of Motor Vehicles), the data are added to a storehouse of personal information about that consumer, which may be sold or shared with third parties. In many of these cases, consumers never explicitly consent to submitting their information to a marketing organization.

Online marketers cannot capture personal information, such as names, addresses, and Social Security numbers, unless people provide them. Without this information, companies can't contact individuals who visit their websites. Data gathered about a user's web browsing through the use of cookies are anonymous, as long as the network advertiser doesn't link the data with personal information. However, if a visitor to a website volunteers' personal information, a website operator can use it to find additional personal information that the visitor may not want to disclose. For example, a name and address can be used to find a corresponding phone number, which can then lead to obtaining even more personal data. All these information become extremely valuable to the website operator, who is trying to build a relationship with website visitors and turn them into customers. The operator can use these data to initiate contact or sell it to other organizations with which they have marketing agreements.

Opponents of consumer profiling are concerned that personal data are being gathered and sold to other companies without the permission of consumers who provide the data. After the data have been collected, consumers have no way of knowing how it is used or who is using it. In fact, consumer data privacy has grown into a major marketing issue. Companies that can't protect or don't respect customer information often lose business, and some become defendants in class action lawsuits stemming from privacy violations.

Electronic Discovery

Electronic discovery (e-discovery) is the collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings. Electronically stored information (ESI) includes any form of digital information, including emails, drawings, graphs, web pages, photographs, word-processing files, sound recordings, and databases stored on any form of magnetic storage device, including hard drives, CDs, and flash drives. Through the e-discovery process, it is quite likely that various forms of ESI of a private or personal nature (e.g., personal emails) will be disclosed.

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. The purpose of discovery is to ensure that all parties go to trial with as much knowledge as possible. Under the rules of discovery, neither party is able to keep secrets from the other. Should a discovery request be objected to, the requesting party may file a motion to compel discovery with the court.

The Federal Rules of Procedure define certain processes that must be followed by a party involved in a case in federal court. Under these rules, once a case is filed, the involved parties are required to meet and discuss various e-discovery issues, such as how to preserve discoverable data, how the data will be produced, agreement on the format in which the data will be provided, and whether production of certain ESI will lead to waiver of attorney–client privilege.

Often organizations will send a litigation hold notice that informs its employees (or employees or officers of the opposing party) to save relevant data and to suspend data that might be due to be destroyed based on normal data-retention rules.

Apple and Samsung were embroiled in a dispute involving alleged patent infringement, which led to an additional dispute over litigation hold notices. During the patent infringement litigation, the court cited Samsung for failing to circulate a comprehensive litigation hold instruction among its employees when it first anticipated litigation.

According to the court, this failure resulted in the loss of emails from several key Samsung employees. Samsung then raised the same issue—Apple had neglected to implement a timely and comprehensive litigation hold to prevent broad destruction of pertinent email. A key learning from

this case is that an organization should focus on its own ESI preservation and production efforts before it raises issues with its opponent's efforts.

Collecting, preparing, and reviewing the tremendous volume of ESI kept by an organization can involve significant time and expense. E-discovery is further complicated because there are often multiple versions of information (such as various drafts) stored in many locations (such as the hard drives of the creator and anyone who reviewed the document, multiple company file servers, and backup tapes). As a result, e-discovery can become so expensive and time consuming that some cases are settled just to avoid the costs.

Workplace Monitoring

Cyberloafing is defined as using the Internet for purposes unrelated to work such as posting to Facebook, sending personal emails or Instant messages, or shopping online. It is estimated that cyberloafing costs U.S. business as much as $85 billion a year. Some surveys reveal that the least productive workers cyberloaf more than 60 percent of their time at work.

Many organizations have developed policies on the use of IT in the workplace in order to protect against employee's abuses that reduce worker productivity or that expose the employer to harassment lawsuits. For example, an employee may sue his or her employer for creating an environment conducive to sexual harassment if other employees are viewing pornography online while at work and the organization takes no measures to stop such viewing. (Email containing crude jokes and cartoons or messages that discriminate against others based on gender, race, sexual orientation, religion, or national origin can also spawn lawsuits.) By instituting and communicating a clear IT usage policy, a company can establish boundaries of acceptable behavior, which enable management to take action against violators.

The potential for decreased productivity and increased legal liabilities has led many employers to monitor workers to ensure that corporate IT usage policies are being followed. Almost 80 percent of major companies choose to record and review employee communications and activities on the job, including phone calls, email, and web surfing. Some are even videotaping employees on the job. In addition, some companies employ random drug testing and psychological testing. With few exceptions, these increasingly common (and many would say intrusive) practices are perfectly legal.

Advanced Surveillance Technology

A number of advances in information technology—such as surveillance cameras and satellite-based systems that can pinpoint a person's physical location—provide amazing new data-gathering capabilities. However, these advances can also diminish individual privacy and complicate the issue of how much information should be captured about people's private lives.

Camera Surveillance

Surveillance cameras are used in major cities around the world in an effort to deter crime and terrorist activities. Critics believe that such scrutiny is a violation of civil liberties and are concerned about the cost of the equipment and people required to monitor the video feeds. Surveillance camera supporters offer anecdotal data that suggest the cameras are effective in preventing crime and terrorism. They can provide examples in which cameras helped solve crimes by corroborating the testimony of witnesses and helping to trace suspects.

Vehicle Event Data Recorders

A vehicle event data recorder (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. Sensors located around the vehicle capture and record information about vehicle speed and acceleration; seat belt usage; air bag deployment; activation of any automatic collision notification system; and driver inputs such as brake, accelerator, and turn signal usage.78 The EDR cannot capture any data that could identify the driver of the vehicle. Nor can it tell if the driver was operating the vehicle under the influence of drugs or alcohol.

The U.S. government does not require EDRs in passenger vehicles. Vehicle manufacturers voluntarily elect to install EDRs, and the capabilities of EDRs vary from manufacturer to manufacturer. If fact, most vehicle owners don't know whether or not their vehicle has an EDR. Beginning with model year 2011 vehicles, the National Highway Traffic Safety Administration (NHTSA) defined a minimum set of 15 data elements that must be captured for manufacturers who voluntarily install EDRs on their vehicles. These data can be downloaded from the EDR and be used for analysis.

One purpose of the EDR is to capture and record data that can be used by the manufacturer to make future changes to improve vehicle performance in the event of a crash. Another purpose is for use in a court of law to determine what happened during a vehicle accident.

Stalking Apps

Technology has made it easy for a person to track the whereabouts of someone else at all times, without ever having to follow the person. Cell phone spy software called a stalking app can be loaded onto someone's cell phone or smartphone within minutes, making it possible for the user to perform location tracking, record calls, view every text message or picture sent or received, and record the URLs of any website visited on the phone. A built-in microphone can be activated remotely to use as a listening device even when the phone is turned off.81 All information gathered from such apps can be sent to the user's email account to be accessed live or at a later time. Some of the most popular spy software includes Mobile Spy, ePhoneTracker, FlexiSPY, and Mobile Nanny.

First Amendment Rights:

The Internet enables a worldwide exchange of news, ideas, opinions, rumours, and information. Its broad accessibility, open discussions, and anonymity make the Internet a remarkable communications medium. It provides an easy and inexpensive way for a speaker to send a message to a large audience—potentially thousands or millions of people worldwide. In addition, given the right email addresses, a speaker can aim a message with laser accuracy at a select subset of powerful and influential people.

People must often make ethical decisions about how to use such incredible freedom and power. Organizations and governments have attempted to establish policies and laws to help guide people, as well as to protect their own interests. Businesses, in particular, have sought to conserve corporate network capacity, avoid legal liability, and improve worker productivity by limiting the non-business use of IT resources.

FIGURE 5-1 The U.S. Constitution

The right to freedom of expression is one of the most important rights for free people everywhere. The First Amendment to the U.S. Constitution (shown in Figure 5-1) was adopted to guarantee this right and others. Over the years, a number of federal, state, and local laws have been found unconstitutional because they violated one of the tenets of this amendment.

The First Amendment reads as follows:

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

In other words, the First Amendment protects Americans' **rights to freedom of religion, freedom of expression, and freedom to assemble peaceably.** This amendment has been interpreted by the Supreme Court as applying to the entire federal government, even though it only expressly refers to Congress.

Numerous court decisions have broadened the definition of speech to include non-verbal, visual, and symbolic forms of expression, such as flag burning, dance movements, and hand gestures. Sometimes the speech at issue is unpopular or highly offensive to a majority of people; however, the Bill of Rights provides protection for minority views. The Supreme Court has also ruled that the First Amendment protects the right to speak anonymously as part of the guarantee of free speech.

The Supreme Court has held that the following types of speech are not protected by the First Amendment and may be forbidden by the government: perjury, fraud, defamation, obscene speech, incitement of panic, incitement to crime, "fighting words," and sedition (incitement of discontent or rebellion against a government).

Two of these types of speech—obscene speech and defamation—are particularly relevant to information technology.

Obscene Speech

Miller v. California is the 1973 Supreme Court case that established a test to determine if material is obscene and therefore not protected by the First Amendment. After conducting a mass mailing campaign to advertise the sale of adult material, Marvin Miller was convicted of violating a California statute prohibiting the distribution of obscene material.

Some unwilling recipients of Miller's brochures complained to the police, initiating the legal proceedings. Although the brochures contained some descriptive printed material, they primarily consisted of pictures and drawings explicitly depicting men and women engaged in sexual activity. In ruling against Miller, the Supreme Court determined that speech can be considered obscene and not protected under the First Amendment based on the following three questions:

- Would the average person, applying contemporary community standards, find that the work, taken as a whole, appeals to the prurient interest?
- Does the work depict or describe, in a patently offensive way, sexual conduct specifically defined by the applicable state law?
- Does the work, taken as a whole, lack serious literary, artistic, political, or scientific value?

Defamation

The right to freedom of expression is restricted when the expressions, whether spoken or written, are untrue and cause harm to another person. Making either an oral or a written statement of alleged fact that is false and that harms another person is defamation. The harm is often of a financial nature, in that it reduces a person's ability to earn a living, work in a profession, or run for an elected office, for example. An oral defamatory statement is slander, and a written defamatory statement is libel. Because defamation is defined as an untrue statement of fact, truth is an absolute defense against a charge of defamation. Although people have the right to express opinions, they must exercise care in their online communications to avoid possible charges of defamation. Organizations must also be on their guard and be prepared to take action in the event of libelous attacks against them.

Freedom Expressions: Key Issues;

Information technology has provided amazing new ways for people to communicate with others around the world, but with these new methods come new responsibilities and new ethical dilemmas.

The number of key issues related to the freedom of expression are…

1. Access to information on the Internet,
2. Internet censorship,
3. SLAPP lawsuits,
4. anonymity on the Internet,
5. John Doe lawsuits,
6. hate speech,
7. pornography on the Internet, and
8. fake news reporting.

1.Controlling Access to Information on the Internet

Although there are clear and convincing arguments to support freedom of speech online, the issue is complicated by the ease with which children can access the Internet. Even some advocates of free speech acknowledge the need to restrict children's Internet access, but it is difficult to restrict their access without also restricting adults' access. In attempts to address this issue, the U.S. government has passed laws, and software manufacturers have invented special software to block access to objectionable material.

The following sections summarize these approaches.

Communications Decency Act

The Telecommunications Act (Public Law 104-104) became law in 1996. Its primary purpose was to allow free competition among phone, cable, and TV companies. The act was broken into seven major sections or titles. Title V of the Telecommunications Act was the Communications Decency Act (CDA), aimed at protecting children from pornography. The CDA

imposed $250,000 fines and prison terms of up to two years for the transmission of "indecent" material over the Internet.

In February 1996, the American Civil Liberties Union (ACLU) and 18 other organizations filed a lawsuit challenging the criminalization of so-called indecency on the web under the CDA. The problem with the CDA was its broad language and vague definition of indecency, a standard that was left to individual communities to determine.

In June 1997, the Supreme Court ruled the law unconstitutional and declared that the Internet must be afforded the highest protection available under the First Amendment. The Supreme Court said in its ruling that "the interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship." The ruling applied essentially the same free-speech protections to communication over the Internet as exist for print communication.

If the CDA had been judged constitutional, it would have opened all aspects of online content to legal scrutiny. Many current websites would probably either not exist or would look much different today had the law not been overturned. Websites that might have been deemed indecent under the CDA would be operating under an extreme risk of liability.

Section 230 of the CDA, which was not ruled unconstitutional, states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" . This provides immunity to an Internet service provider (ISP) that publishes user generated content, as long as its actions do not rise to the level of a content provider. In general, the closer an ISP is to a pure service provider than to a content provider, the more likely that the Section 230 immunity will apply. This portion of the CDA protects social networking companies such as Facebook and Twitter from defamation suits in connection with user postings that appear on their sites.

Facebook presents a constantly updated list of stories, called the News Feed, in the middle of each Facebook user's home page. Using an algorithm based on each user's Facebook activity and connections, the social networking site attempts to choose the "best" content out of several thousand potential stories, placing those near the top of the News Feed. The number of comments and likes a post receives, as well as what type of story it is (e.g., photo, video, news article, or status update), influences whether and how prominently a story will appear in a user's News Feed. Facebook also conducts surveys and focus groups to get input on what stories people think should appear. The more engaging the content, the more time users will spend on Facebook and the more often they will likely return to the site. This enables Facebook to earn more revenue from ads shown in News Feed content.

Because one of the traditional roles of a publisher is to select which stories to show its readers, Facebook's efforts to shape the news that its users see could result in it being viewed as an

information content provider by the courts, resulting in a loss of protection under Section 230 of the CDA. If that were to happen, Facebook could become liable for defamation based on the postings of its subscribers.

Child Online Protection Act

In October 1998, the Child Online Protection Act (COPA) was signed into law. This act is not to be confused with the Children's Online Privacy Protection Act (COPPA) that is directed at websites that want to gather personal information from children under the age of 13. COPA states that "whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both."

Internet Filtering

An Internet filter is software that can be used to block access to certain websites that contain material deemed inappropriate or offensive. The best Internet filters use a combination of URL, keyword, and dynamic content filtering. With URL filtering, a particular URL or domain name is identified as belonging to an objectionable site, and the user is not allowed access to it. Keyword filtering uses keywords or phrases—such as sex, Satan, and gambling—to block websites. With dynamic content filtering, each website's content is evaluated immediately before it is displayed, using techniques such as object analysis and image recognition.

The negative side of Internet filters is that they can block too much content, keeping users from accessing useful information about civil rights, health, sex, and politics as well as online databases and online book catalogs.

Some organizations choose to install filters on their employees' computers to prevent them from viewing sites that contain pornography or other objectionable material. Employees unwillingly exposed to such material would have a strong case for sexual harassment. The use of filters can also ensure that employees do not waste their time viewing nonbusiness-related websites.

Children's Internet Protection Act

In another attempt to protect children from accessing pornography and other explicit material online, Congress passed the Children's Internet Protection Act (CIPA) in 2000. The act required federally financed schools and libraries to use some form of technological protection (such as an Internet filter) to block computer access to obscene material, pornography, and anything else considered harmful to minors.

Congress did not specifically define what content or websites should be forbidden or what measures should be used— these decisions were left to individual school districts and library systems. Any school or library that failed to comply with the law would no longer be eligible to

receive federal money through the E-Rate program, which provides funding to help pay for the cost of Internet connections. The following points summarize CIPA:

- •Under CIPA, schools and libraries subject to CIPA will not receive the discounts offered by the E-Rate program unless they certify that they have certain Internet safety measures in place to block or filter pictures that are obscene, contain child pornography, or are harmful to minors (for computers used by minors).
- Schools subject to CIPA are required to adopt a policy to monitor the online activities of minors.
- Schools and libraries subject to CIPA are required to adopt a policy addressing access by minors to inappropriate matter online; the safety and security of minors when using email, chat rooms, and other forms of direct electronic communications; unauthorized access, including hacking and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal information regarding minors; and restricting minors' access to materials harmful to them. CIPA does not require the tracking of Internet use by minors or adults.

Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA), which was signed into law in 1998, addresses a number of copyright-related issues. The DMCA is divided into five title among this Title II, the "Online Copyright Infringement Liability Limitation Act," provides limitations on the liability of an ISP for copyright infringement that can arise when an ISP subscriber posts copyrighted material such as audio tracks, videos, books, and news articles on the Internet.

Its passage amended Title 17 of the U.S. Code (Copyright) by adding a new Section 512, which says that an ISP cannot be held liable for copyright infringement if, when notified by the copyright holder, it notifies the subscriber of the alleged infringement and executes a "takedown" by removing the offending content. The fact that the content was created by you, or in the case of a photo or video the subject is you, can be sufficient enough to request a takedown.

2.Internet Censorship

Internet censorship is the control or suppression of the publishing or accessing of information on the Internet.

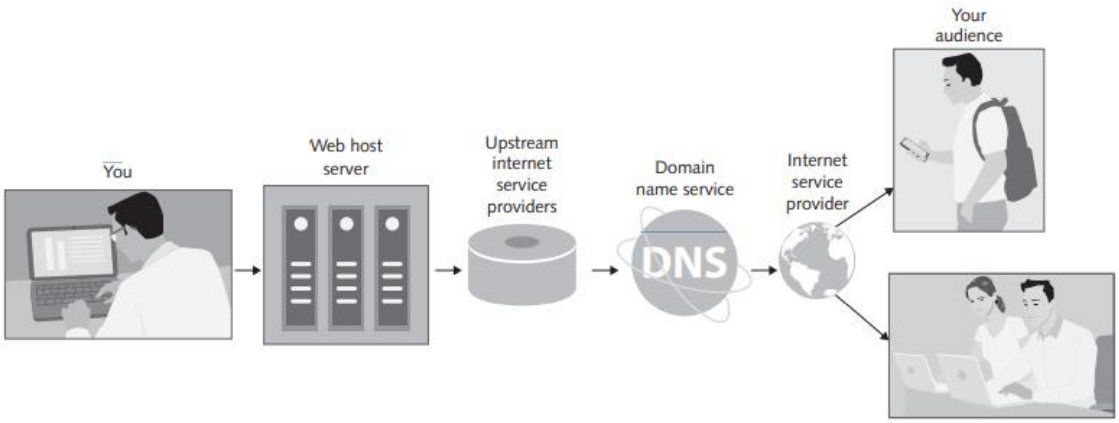

FIGURE 5-3 Internet Censorship

Speech on the Internet requires a series of intermediaries to reach its audience (see Figure 5-3) with each intermediary vulnerable to some degree of pressure from those who want to silence the speaker. Web hosting services are often the recipients of defamation or copyright infringement claims by government authorities or copyright holders, demanding the immediate takedown of hosted material that is deemed inappropriate or illegal.

Government entities may pressure "upstream" Internet service providers to limit access to certain websites, allow access to only some content or modified content at certain websites, reject the use of certain keywords in search engines, and track and monitor the Internet activities of individuals. Several countries have enacted the so-called three-strikes laws that require ISPs to terminate a user's Internet connection once that user has received a number of notifications of posting of content deemed inappropriate or illegal.

Censorship efforts may also focus on Domain Name System (DNS) servers, which convert human-readable host and domain names into the machine-readable, numeric Internet Protocol (IP) addresses that are used to point computers and other devices toward the correct servers on the Internet. Where authorities have control over DNS servers, officials can "deregister" a domain that hosts content that is deemed inappropriate or illegal so that the website is effectively invisible to users seeking access to the site.

3.SLAPP lawsuits

A strategic lawsuit against public participation (SLAPP) is employed by corporations, government officials, and others against citizens and community groups who oppose them on matters of public interest. The lawsuit is typically without merit and is used to intimidate critics out of fear of the cost and efforts associated with a major legal battle. Many question the ethics and legality of using a SLAPP; others claim that all is fair when it comes to politics and political issues.

Of course, the plaintiff in a SLAPP cannot present themselves to the court admitting that their intent is to censor their critics. Instead, the SLAPP takes some other form, such as a defamation lawsuit that make claims with vague wording that enables plaintiffs to make bogus accusations without fear of perjury. The plaintiff refuses to consider any settlement and initiates an endless stream of appeals and delays in an attempt to drag the suit out and run up the legal costs.

Every year thousands of people become SLAPP victims while participating in perfectly legal actions such as phoning a public official, writing a letter to the editor of a newspaper, speaking out at a public meeting, posting an online review, or circulating a petition.

1. SLAPPs are Strategic Lawsuits Against Public Participation. These damaging suits chill free speech and healthy debate by targeting those who communicate with their government or speak out on issues of public interest.
2. SLAPPs are used to silence and harass critics by forcing them to spend money to defend these baseless suits. SLAPP filers don't go to court to seek justice. Rather, SLAPPS are intended to intimidate those who disagree with them or their activities by draining the target's financial resources.
3. SLAPPs are effective because even a meritless lawsuit can take years and many thousands of dollars to defend. To end or prevent a SLAPP, those who speak out on issues of public interest frequently agree to muzzle themselves, apologize, or "correct" statements.

For example, an unhappy home owner wrote two scathing reviews on Yelp when the contractor he had hired to install a new hardwood floor botched the job. For six months, the homeowner and contractor tried to work things out but to no avail. The contractor sued the home owner for civil theft, intentional interference, and defamation claiming the online reviews had caused it to lose $625,000 worth of business and demanded $125,000 in compensation. The home owner eventually removed the reviews, but only after spending $60,000 on legal fees plus another $15,000 to settle the case. The contractor insisted that its suit wasn't a SLAPP because it was filed months after the reviews were posted, was primarily about the homeowner's failure to pay, and involved a legitimate defamation claim.

Anti-SLAPP laws are designed to reduce frivolous SLAPPs. As of 2015, 28 states and the District of Columbia had passed anti-SLAPP legislation to protect people who are the target of a SLAPP. Typically, under such legislation, a person hit with what they deem to be a SLAPP can quickly file an anti-SLAPP motion, which puts a hold on the original lawsuit until the court determines whether the defendant was being targeted for exercising free-speech rights, petitioning the government, or speaking in a public forum on "an issue of public interest." In such cases, the SLAPP lawsuit is thrown out unless the plaintiff can show that the claims are legitimate and likely to succeed at trial. To guard against abusive anti-SLAPP motions, the side that loses such a case is required to pay the other side's legal fees.

4.Anonymity on the Internet

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. However, in the wrong hands, anonymous communication can be used as a tool to commit illegal or unethical activities.

Anonymous political expression played an important role in the early formation of the United States. Before and during the American Revolution, patriots who dissented against British rule often used anonymous pamphlets and leaflets to express their opinions.

England had a variety of laws designed to restrict anonymous political commentary, and people found guilty of breaking these laws were subject to harsh punishment—from whippings to hangings. A famous case in 1735 involved a printer named John Zenger, who was prosecuted for seditious libel because he wouldn't reveal the names of anonymous authors whose writings he published. The authors were critical of the governor of New York. The British were outraged when the jurors refused to convict Zenger, in what is considered a defining moment in the history of freedom of the press in the United States.

Other democracy supporters often authored their writings anonymously or under pseudonyms. For example, Thomas Paine was an influential writer, philosopher, and statesman of the Revolutionary War era. He published a pamphlet called Common Sense, in which he criticized the British monarchy and urged the colonies to become independent by establishing a republican government of their own. Published anonymously in 1776, the pamphlet sold more than 500,000 copies, at a time when the population of the colonies was estimated to have been less than four million; it provided a stimulus to produce the Declaration of Independence six months later.

Despite the importance of anonymity in early America, it took nearly 200 years for the Supreme Court to render rulings that addressed anonymity as an aspect of the Bill of Rights. One of the first rulings was in the 1958 case of National Association for the Advancement of Colored People (NAACP) v. Alabama, in which the court ruled that the NAACP did not have to turn over its membership list to the state of Alabama. The court believed that members could be subjected to threats and retaliation if the list were disclosed and that disclosure would restrict a member's right to freely associate, in violation of the First Amendment.

5.John Doe Lawsuits

Businesses must monitor and respond to both the public expression of opinions that might hurt their reputations and the public sharing of confidential company information. When anonymous employees reveal harmful information online, the potential for broad dissemination is enormous, and it can require great effort to identify the people involved and stop them.

An aggrieved party can file a John Doe lawsuit against a defendant whose identity is temporarily unknown because he or she is communicating anonymously or using a pseudonym. Once the John

Doe lawsuit is filed, the plaintiff can request court permission to issue subpoenas to command a person to appear under penalty. If the court grants permission, the plaintiff can serve subpoenas on any third party—such as an ISP or a website hosting firm—that may have information about the true identity of the defendant. When, and if, the identity becomes known, the complaint is modified to show the correct name(s) of the defendant(s). This approach is also frequently employed in copyright infringement lawsuits where unknown parties have downloaded movies or music from the Internet.

ISPs—such as AT&T, Comcast, and CenturyLink—and social networking sites—such as Facebook and Pinterest—receive more than a thousand subpoenas per year directing them to reveal the identity of John Does. Free-speech advocates argue that if someone charges libel, the anonymity of the web poster should be preserved until the libel is proved. Otherwise, the subpoena power can be used to silence anonymous, critical speech.

Proponents of such lawsuits point out that most John Doe cases are based on serious allegations of wrongdoing, such as libel or disclosure of confidential information. For example, stock price manipulators can use chat rooms to affect the share price of stocks— especially those of very small companies that have just a few outstanding shares. In addition, competitors of an organization might try to create the feeling that the organization is a miserable place to work, which could discourage job candidates from applying, investors from buying stock, or consumers from buying company products. Proponents of John Doe lawsuits argue that perpetrators should not be able to hide behind anonymity to avoid responsibility for their actions.

Anonymity is not guaranteed. By filing a lawsuit, companies gain immediate subpoena power, and many message board hosts release information as soon as it is requested, often without notifying the poster. Everyone who posts comments in a public place on the web should consider the consequences if their identities were to be exposed. Furthermore, everyone who reads anonymous postings online should think twice about believing what they read.

The California State Court in Pre-Paid Legal v. Sturtz et al.28 set a legal precedent that refined the criteria the courts apply when deciding whether or not to approve subpoenas requesting the identity of anonymous web posters. The case involved a subpoena issued by Pre-Paid Legal Services (PPLS), which requested the identity of eight anonymous posters on Yahoo's Prepaid message board. Attorneys for PPLS argued that the company needed the posters' identities to determine whether they were subject to a voluntary injunction that prevented former sales associates from revealing PPLS's trade secrets.

The EFF represented two of the John Does whose identities were subpoenaed. EFF attorneys argued that the message board postings cited by PPLS revealed no company secrets but were merely disparaging the company and its treatment of sales associates. They argued further that requiring the John Does to reveal their identities would let the company punish them for speaking out and set a dangerous precedent that would discourage other Internet users from voicing

criticism. Without proper safeguards on John Doe subpoenas, a company could use the courts to uncover its critics.

EFF attorneys urged the court to apply the four-part test adopted by the federal courts in Doe v. 2TheMart.com, Inc. 29 to determine whether a subpoena for the identity of the web posters should be upheld. In that case, the federal court ruled that a subpoena should be enforced only when the following occurs:

- The subpoena was issued in good faith and not for any improper purpose.
- The information sought was related to a core claim or defense.
- The identifying information was directly and materially relevant to that claim or defense.
- Adequate information was unavailable from any other source.

A judge in Santa Clara County Superior Court invalidated the subpoena requesting the posters' identities. He ruled that the messages were not obvious violations of the injunctions invoked by PPLS and that the First Amendment protection of anonymous speech outweighed PPLS's interest in learning the identity of the speakers.

6.Hate Speech

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. Persistent or malicious harassment aimed at a specific person is hate speech, which can be prosecuted under the law, but general, broad statements expressing hatred of an ethnic, racial, or religious group cannot. A threatening private message sent over the Internet to a person, a public message displayed on a website describing intent to commit acts of hate-motivated violence against specific individuals, and libel directed at a particular person are all actions that can be prosecuted.

Although ISPs and social networking sites do not have the resources to prescreen content (and they do not assume any responsibility for content provided by others), many ISPs and social networking sites do reserve the right to remove content that, in their judgment, does not meet their standards. The speed at which content may be removed depends on how quickly such content is called to the attention of the ISP or social networking site, how egregious the content is, and the general availability of the company's resources to handle such issues.

To post videos on YouTube, you must first create a YouTube or a Google account (Google is the owner of YouTube) and agree to abide by the site's published guidelines.30 The YouTube guidelines prohibit the posting of videos showing such things as pornography, animal abuse, graphic violence, predatory behavior, and drug use. The guidelines also prohibit the posting of copyrighted material—such as music, television programs, or movies—that is owned by a third party. YouTube staff members review user-posted videos on a regular basis to find any that violate the site's community guidelines. Those that violate the guidelines are removed. Certain other

videos are age-restricted because of their content. Users are penalized for serious or repeated violations of the guidelines and can have their account terminated.31

7.Pornography on the Internet

Many people, including some free-speech advocates, believe that there is nothing illegal or wrong about purchasing adult pornographic material made by and for consenting adults. They argue that the First Amendment protects such material. On the other hand, most parents, educators, and other child advocates are concerned that children might be exposed to online pornography. They are deeply troubled by its potential impact on children and fear that increasingly easy access to pornography encourages pedophiles and sexual predators.

Clearly, the Internet has been a boon to the pornography industry by providing fast, cheap, and convenient access to many millions of porn websites worldwide.34 Access via the Internet enables pornography consumers to avoid offending others or being embarrassed by others observing their purchases. There is no question that online adult pornography is big business (revenue estimates vary widely between $1 billion and $97 billion) and generates a lot of traffic; it is estimated that there are over 72 million visitors to pornographic websites monthly.35,36

If what someone distributes or exhibits is judged obscene, they are subject to prosecution under the obscenity laws. The precedent-setting Miller v. California ruling on obscenity discussed earlier in the chapter predates the Internet. The judges in that case ruled that contemporary community standards should be used to judge what is obscene. The judges allowed that different communities could have different norms.

The key question in deciding what Internet material is obscene is: "Whose community standards are used?" Because Internet content publishers cannot easily direct their content into or away from a particular geographic area, one answer to this question is that the Internet content publisher must conform to the norms of the most restrictive community. However, this line of reasoning was challenged by the Third Circuit Court of Appeals in the Ashcroft v. American Civil Liberties Union case, which involved a challenge to the 1998 COPA. The Supreme Court reversed the circuit court's ruling in this case—but with five different opinions and no clear consensus on the use of local or national community standards.37 In United States v. Kilbride, the Ninth Circuit Court of Appeals ruled that "a national community standard must be applied in regulating obscene speech on the Internet, including obscenity disseminated via email."38 In United States v. Little, the Eleventh Circuit Court of Appeals rejected the national community standard and adopted the older, local community standard. Currently, there is no clear agreement within the courts on whether local or national community standards are to be used to judge obscenity.

U.S. organizations must be very careful when dealing with issues relating to pornography in the workplace. By providing computers, Internet access, and training in how to use those computers and the Internet, companies could be seen by the law as purveyors of pornography because they have enabled employees to store pornographic material and retrieve it on demand. Nielsen has found that 25 percent of working adults admit to looking at pornography on a computer

at work.39 In addition, if an employee sees a coworker viewing porn on a workplace computer, that employee may be able to claim that the company has created a hostile work environment. Such a claim opens the organization to a sexual harassment lawsuit that can cost hundreds of thousands of dollars and tie up managers and executives in endless depositions and court appearances.

Many companies believe that they have a duty to stop the viewing of pornography in the workplace. As long as they can show that they took reasonable steps and determined actions to prevent it, they have a valid defense if they become the subject of a sexual harassment lawsuit. If it can be shown that a company made only a half-hearted attempt to stop the viewing of pornography in the workplace, then the company could have trouble defending itself in court. Reasonable steps include establishing and communicating an acceptable use policy that prohibits access to pornography sites, identifying those who violate the policy, and taking disciplinary action against those who violate the policy, up to and including termination.

A few companies take the opposite viewpoint—that they cannot be held liable if they don't know employees are viewing, downloading, and distributing pornography. Therefore, they believe the best approach is to ignore the problem by never investigating it, thereby ensuring that they can claim that they never knew it was happening. Many people would consider such an approach unethical and would view management as shirking an important responsibility to provide a work environment free of sexual harassment. Employees unwillingly exposed to pornography would have a strong case for sexual harassment because they could claim that pornographic material was available in the workplace and that the company took inadequate measures to control the situation.

Numerous federal laws address issues related to child pornography—including laws concerning the possession, production, distribution, or sale of pornographic images or videos that exploit or display children. Possession of child pornography is a federal offense punishable by up to five years in prison. The production and distribution of such materials carry harsher penalties; decades or even life in prison is not an unusual sentence. In addition to these federal statutes, all states have enacted laws against the production and distribution of child pornography, and all but a few states have outlawed the possession of child pornography. At least seven states have passed laws that require computer technicians who discover child pornography on clients' computers to report it to law enforcement officials.

Sexting—sending sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone—is a fast-growing trend among teens and young adults. A Drexel University survey of college students revealed that 54 percent had sent or received "sexually explicit text messages or images" when they were under age 18. Previous studies had pegged the number much lower—around 20 percent. Students in this study may have been more honest because they were allowed to remain anonymous and were reporting on past behavior.

Increasingly, people who take part in sexting are suffering the consequences of this fad. Once an image or video is sent, there is no taking it back and no telling to whom it might be

forwarded. And it is not just teenagers who participate in sexting. Consider quarterback Bret Favre and U.S. representative Anthony Weiner who were both parties to embarrassing sexting episodes. Sexters can also face prosecution for child pornography, leading to possible years in jail and decades of registration as a sex offender. Some states have adopted laws that prescribe penalties aimed specifically at teenagers engaged in sexting. These laws make the penalties for teen sexting less severe than if an adult would send similar photos to an under-age person

8.Fake news reporting.

Fake News Journalism, including the ways in which people get their news, is going through a period of rapid change. The sale of traditional newspapers and magazines continues to fall while online consumption of news is growing. Nearly twice as many adults (38 percent) report that they often get news online rather than from print media (20 percent). Much online news continues to come from traditional news sources, such as ABC, CBS, CNN, Fox, and NBC news, the Chicago Tribune, the New York Times, Newsweek, the Wall Street Journal, and U.S. News & World Report. However, readers looking for news and information online will also find a wide range of non-traditional sources—some of which offer more objective, verifiable news reporting than others—including the following types:

- **Blogs—**On some blogs, writers discuss news and editorial content produced by other journalists and encourage reader participation. Bloggers often report on things about which they are very passionate. As a result, they may be less likely to remain unbiased, instead stating their opinion and supporting facts without presenting the other side of an argument. Indeed, many bloggers pride themselves on their lack of objectivity, instead viewing themselves as an activist for a particular cause or point of view.
- **Fake news sites—**These sites attempt to imitate real news sites, often modifying real news stories in such a way as to entice viewers into clicking on them. In other cases, fake news sites simply create entirely fictitious "news" stories and present them as fact. In many cases, readers of online news simply glance at headlines or skim an article without ever realizing it is fake or distorted news. Indeed, almost a quarter of Americans admit to sharing fake news, and about two-thirds say that fake news has caused "a great deal of confusion" about current events.
- **Social media sites—**Ordinary citizens are increasingly involved in the collection, reporting, analysis, and dissemination of news, opinions, and photos, which are then posted to various social media sites. Often, citizen journalists are "on the spot" and able to report on breaking news stories before traditional news reporters. While such timeliness of reporting can be a good thing, it does not always promote accuracy, clarity, and objectivity. Because reports, images, opinions, and videos shared via social media often spread like wildfire, they can sometimes cause confusion, misunderstanding, and controversy, rather than bringing clarity to a situation.

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. Headlines from such "fake news" stories in 2016 include "Pope Francis shocks world, endorses Donald Trump for president," "WikiLeaks confirms Hillary sold weapons to ISIS," and "FBI agent suspected in Hillary email leaks found dead in apparent murder-suicide." Critics of such sites argue that real journalists adhere to certain standards, such as fact checking, identifying and verifying sources, presenting opinions on both sides of an issue, and avoiding libellous statements. While there are many legitimate online journalists who produce high-quality, evidence-based reporting, too often, online reporting stresses immediacy, speed, sensationalism, and the need for post-publication correction.

Social Networking Ethical Issues

Some common ethical issues that arise for members of social networking platforms are online abuse, harassment, stalking, cyberbullying, encounters with sexual predators, the uploading of inappropriate material, and the participation of employees in social networking. Additional social networking issues include 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.

Cyber-abuse, Cyber-harassment, and Cyberstalking

Cyber-abuse

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. Cyberabuse encompasses both cyberharassment and cyberstalking, a broad spectrum of behaviors wherein someone acts in a way that causes harm and distress to others.

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.

Here are a few tips to help you avoid becoming a victim of cyberabuse:

- **Always use a strong, unique password** (12-plus characters, including a mix of numbers, capital letters, and special characters) for each social networking site.
- If you broke up with an intimate partner, reset the passwords on all of your accounts, including email, financial, and social networking accounts.
- Check your privacy settings to ensure that you are sharing only the information you want to share with only people you trust and not the general Internet public.
- Some sites have options for you to test how your profile is being viewed by others—use this feature to make sure you only reveal what is absolutely necessary.

- Warn your friends and acquaintances not to post personal information about you, especially your contact information and location.
- Don't post photographs of your home that might indicate its location by showing the street address or a nearby identifying landmark.
- If you connect your smartphone to your online account, do not provide live updates on your location or activities.
- Avoid posting information about your current or future locations.
- Do not accept "friend requests" from strangers.
- Avoid online polls, quizzes, or surveys that ask for personal information.

Cyberstalking

Cyberstalking is a subcategory of cyberabuse that consists of a long-term pattern of unwanted, persistent pursuit and intrusive behaviour (involving the use of an electronic communications device) that is directed by one person against another and that causes fear and distress in the victim. Occasionally, cyberstalkers are complete strangers, but it is more common for victims to know the stalker.

Cyberstalking can be a serious problem for victims, terrifying them and causing mental anguish. It is not unusual for cyberstalking to escalate into abusive or excessive phone calls, threatening or obscene mail, trespassing, vandalism, physical stalking, and even physical assault.

Table 9-4 provides examples of cyberharassment and cyberstalking.

TABLE 9-4 Examples of cyberharassment and cyberstalking

Cyberharassment	Cyberstalking	Neither
Someone keeps sending you instant messages after you have asked them to stop.	Someone sends you a credible threat that they are "out to get you."	Someone posts a strongly worded dissenting opinion to your post on a social network.
Someone posts a message in such a manner that it appears to have come from you.	An unknown individual keeps sending you messages like, "I saw you at….": the messages name specific locations you have been.	Someone posts a message disparaging members of a particular race, ethnic group, or sexual orientation to which you belong.
Someone posts explicit or embarrassing photos or videos of you (revenge porn) without your permission.	An unknown individual posts photos of you taken over several days in different locations, without you even being aware that your photo was taken.	

Encounters with Sexual Predators

Some social networking platforms, law enforcement, and the courts have been criticized for not doing enough to protect minors from encounters with sexual predators. Most law enforcement officers understand that dangers exist in not mandating Internet restrictions for repeat sex offenders but also realize that creating a national policy would be difficult because even convicted felons have first amendment rights.

The 1994 Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act set the initial requirements for sex offender registration and notification in the United States. The act requires sex offenders to register their residence with local law enforcement agencies. It also required that states create websites that provide information on sex offenders within the state.

The goal of the act was to provide law enforcement and citizens with the location of all sex offenders in the community. However, which sex offenders and what data would appear on the websites was left to the various states to decide. Because of the lack of consistency among the various states, the act was less effective than desired, and sex offenders sometimes simply moved to states with less strict reporting requirements to avoid registering. The act was named after an 11-year-old Minnesota boy who was abducted and murdered in 1989.

Uploading of Inappropriate Material

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 site. Typically, the terms state that the site has the right to delete the material and terminate user accounts that violate the site's policies. The policies set specific limits on content that is sexually explicit, defamatory, hateful, violent, or that promotes illegal activity.

Policies do not stop all members of the community from attempting to post inappropriate material, and Section 230 of the Communications Decency Act protects a website from certain liabilities resulting from the publication of objectionable materials posted by the users of that website. Most sites do not have sufficient resources to review all materials submitted for posting. For example, more than 400 hours of content are uploaded to YouTube every minute. Quite often, it is only after other members of a social networking site complain about objectionable material that such material is taken down. This can be days or even weeks.

Inappropriate material posted online includes non-consensual posts that comprise 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. Revenge porn content is sometimes linked to the person's other online accounts, such as Facebook, LinkedIn, or even an employer's website, along with personal information including addresses and telephone numbers. In this context, revenge porn can be considered a form of domestic abuse and stalking.

In March 2017, a report revealed that more than 2,500 photos of female Marines in various stages of undress or engaging in sexual acts had been posted to a closed Facebook group (called Marines United) with more than 30,000 members. One month after discovery of the material, Facebook announced that it would modify its procedures for dealing with such material. In the future, when such content is reported to Facebook, a trained member of its community standards team will review it. If deemed in violation of the terms of the user agreement, the content will be removed and the account of the individual who posted it will be disabled. Facebook will employ artificial intelligence and image recognition to identify and prevent the posting of similar images in Facebook, Messenger, and Instagram.

Employee Participation on Social Media Networks

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. So, while state and federal government employees have protection from retaliation for exercising certain First Amendment rights, some 18 percent of private employers surveyed say they have dismissed employees because of something they posted on social media.

In 2016, a woman posted an expletive-laden, racist rant on her personal Facebook page. After another Facebook user checked her Facebook profile and discovered that she was a Bank of America employee, the bank received thousands of phone calls and social media comments challenging the hateful post. Her managers learned of the post one day, investigated, and fired her the next day for her inexcusable comments.

Organizations should put in place a social media policy to avoid legal issues and set clear guidelines and expectations for employees. With a policy in place, employees can feel empowered to exercise creativity and express their opinions without concern that what they are sharing on social media could negatively impact their career.

Miscellaneous Social Media Issues

Although many drivers believe that talking on a phone does not affect their driving, studies found that this activity quadruples your risk of an accident to about the same level as if you were driving drunk! That risk doubles again, to eight times normal, if you are texting.

Social media brings out the narcissist tendencies of users driving them to go on and on about how great their life is and all the wonderful things they are doing. Such postings paint an unrealistic picture of the individual and become tedious to many while others may become discouraged that their lives are not as interesting.

Social media platforms also enable a degree of self-image manipulation. For example, Snapchat provides filters that alter the user's face by smoothing and whitening skin, changing eye shape, nose size, and jaw profile. Some users favor the filters because they enable users to feel more

confident posting their photo while others feel that the filters promote an unrealistic and Westernized standard of beauty.

========== End of Unit-3 ==========

Unit 3: Privacy and Freedom of Expression (10 Hrs.)

Privacy Protection and the Law - Information Privacy, Privacy Laws, Applications, and Court Rulings; Key Privacy and Anonymity Issues - Consumer Profiling, Electronic Discovery, Workplace Monitoring, Surveillance; First Amendment Rights; Freedom Expressions: Key Issues; Social Networking Ethical Issues