Privacy & Freedom of Expression

Course Name: Cyber Law & Professional Ethics (3 Cr.)
Course Code: CACS401
Year/Semester: IV/VII
Class Load: 4 Hrs. / Week (Theory: 3Hrs. Tutorial: 1 Hrs.)

Course Description:
This course presents different concepts of cyber law, cybersecurity, and ethics for IT professionals and IT Organizations. This course also presents different concepts related to intellectual properties and their protections, privacy, and social networking issues.

Course Objectives:
The primary objective of this course is to provide knowledge of cyber law, cybersecurity, privacy protection, intellectual property protection, and ethics for IT professionals and IT organizations.

Course Contents:
Unit 1: An Overview of Ethics, Ethics for IT Workers and IT Users (10 Hrs.)
Ethics, Ethics in the Business World; Corporate Social Responsibility; Fostering Corporate Social Responsibility and Good Business Ethics; Improving Business Ethics; Ethical Considerations in Decision Making; Ethics in Information Technology; Managing IT Worker Relationship; Encouraging Professionalism of IT Workers – Professional Codes of Ethics, Professional Organizations, Certifications and Licensing ; Encouraging Ethical Use of IT Resources among Users

Unit 2: Cyberattacks, Cybersecurity, and Cyber Law (12 Hrs.)

Threat Landscape – Computer Incidents, Types of Exploits; CIA Security Triad – Confidentiality, Integrity, Availability, Implementing CIA at Organizational, Network, Application, and End-User Level; Response to Cyberattack - Incident Notification Protection of Evidence and Activity Logs Incident Containment Eradication Incident Follow-Up Using an MSSP, and Computer Forensics; Cyber Law; Provision of Cyber Law and Electronic Transaction Act of Nepal

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

Unit 4: Intellectual Property (8 Hrs.)

Intellectual Property, Copyright; Patient; Trade Secrets; Intellectual Property Issues: Plagiarism, Reverse Engineering, Open Source Code, Competitive Intelligence, Trademark Infringement, and Cybersquatting

Unit 5: Ethical Decision in Software Development and Ethics of IT Organizations (8 Hrs.)

Software Quality and its Importance; Strategies for Developing Quality Software; Use of Contingent Workers; H-1B Workers; Outsourcing; Whistle-Blowing; Green Computing

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, analyzed, and reported because organizations can use it to make better decisions.
- 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.

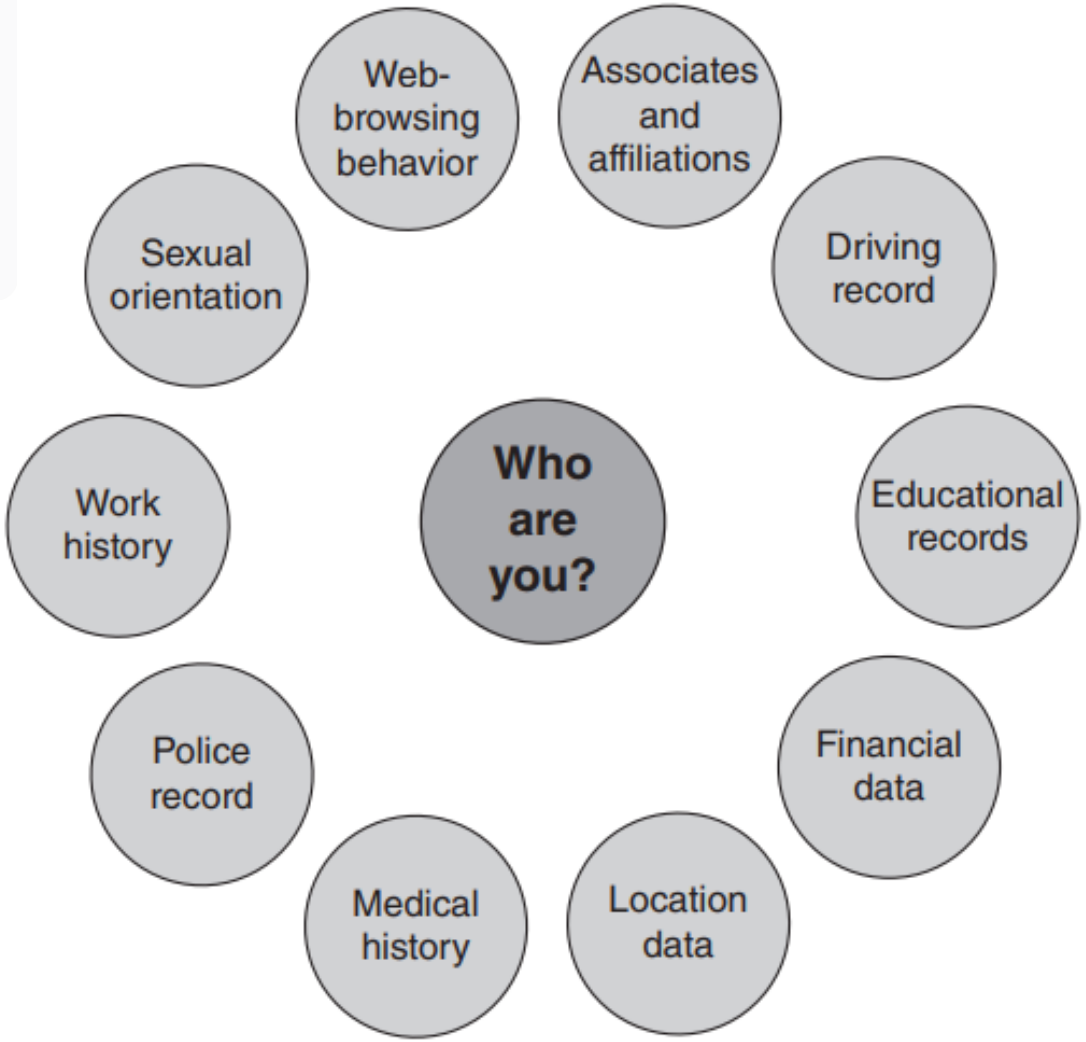

FIGURE 4-1 Organizations gather a variety of data about people in order to make better decisions

- However, many people object to the data collection policies of governments and businesses on the grounds that they strip (remove) individuals of the power to control their own personal information.
- For these people, the existing hodgepodge (a confused mixture) of privacy laws and practices fails to provide adequate protection; rather, it causes confusion that promotes distrust and skepticism (doubt as to the truth of something), which are further fueled by the disclosure of threats to privacy.
- A combination of approaches—new laws, technical solutions, and privacy policies—is 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.

- 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**.

- **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).
- The following sections cover concepts and principles related to information privacy, beginning with a summary of the most significant privacy laws, their applications, and related court rulings.

- **Privacy Laws, Applications, and Court Rulings**
- This section outlines a number of legislative acts that affect a person's privacy.
- Note that most of these actions address invasion (violation/capture) of privacy by the government.
- Legislation that protects people from data privacy abuses by corporations is almost nonexistent.
- Although a number of independent laws and acts have been implemented over time, no single, overarching (comprehensive) 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.
- You can track the status of privacy legislation in the United States at the Electronic Privacy Information Center's website (www.epic.org).

- **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 (inspection/scan) 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).
- The financial institution cannot release a customer's financial records until the government authority seeking the records certifies in writing that it has complied with the applicable provision of the act.

- The act only governs disclosures to the federal government; it does not cover disclosures to private businesses or state and local governments.
- **Gramm-Leach-Bliley Act (1999)**
- The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, was a bank deregulation law that repealed a Depression-era law known as Glass-Steagall.
- Glass-Steagall prohibited any one institution from offering investment, commercial banking, and insurance services; individual companies were only allowed to offer one of those types of financial service products.

- GLBA enabled such entities to merge.
- GLBA also included three key rules that affect personal privacy:
- *Financial Privacy Rule*—This rule established mandatory guidelines for the collection and disclosure of personal financial information by financial organizations. Under this provision, financial institutions must provide a privacy notice to each consumer that explains what data about the consumer are gathered, with whom that data are shared, how the data are used, and how the data are protected. The notice must also explain the consumer's right to opt out—to refuse to give the institution the right to collect and share personal data with unaffiliated parties.

- Anytime the privacy policy is changed, the consumer must be contacted again and given the right to opt out. The privacy notice must be provided to the consumer at the time the consumer relationship is formed and once each year thereafter. Customers who take no action automatically opt in and give financial institutions the right to share personal data, such as annual earnings, net worth, employers, personal investment information, loan amounts, and Social Security numbers, with other financial institutions.

- *Safeguards Rule*—This rule requires each financial institution to document a data security plan describing its preparation and plans for the ongoing protection of clients' personal data.
- *Pretexting Rule*—This rule addresses attempts by people to access personal information without proper authority by means such as impersonating an account holder or phishing. GLBA encourages financial institutions to implement safeguards against pretexting.

- **Fair and Accurate Credit Transactions Act (2003)**
- The Fair and Accurate Credit Transactions Act (Public Law 108-159) 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 (Equifax, Experian, and TransUnion).
- 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.
- For their part, healthcare companies must appoint a privacy officer to develop privacy policies and procedures as well as train employees on how to handle sensitive patient data.
- These actions must address the potential for unauthorized access to data by outside hackers as well as the more likely threat of internal misuse of data.

- The penalties for noncompliance are based on the level of negligence, and violations can also carry criminal charges that can result in jail time.
- New York and Presbyterian Hospital and Columbia University agreed to pay $4.8 million to settle charges that they potentially violated HIPAA regulations by failing to secure thousands of patients' electronic protected health information held on their network.
- **The American Recovery and Reinvestment Act (2009)**
- The American Recovery and Reinvestment Act is a wide-ranging act passed in 2009 that authorized $787 billion in spending and tax cuts over a 10-year period.

- Title XIII, Subtitle D, of this act (known as the Health Information Technology for Economic and Clinical Health Act, or HITECH) included strong privacy provisions for electronic health records (EHRs), including banning the sale of health information, promoting the use of audit trails and encryption, and providing rights of access for patients.
- It also mandated that each individual whose health information has been exposed be notified within 60 days after discovery of a data breach.

- *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.1
- 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 (disclose) personal data; and becoming involved in gambling or other inappropriate behavior.
- 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.
- Under FERPA, the presumption is that a student's records are private and not available to the public without the consent of the student.
- Penalties for violation of FERPA may include a cutoff of federal funding to the educational institution.

- Educational agencies and institutions may disclose education records to the parents of a dependent student, as defined in Section 152 of the Internal Revenue Code of 1986, without the student's consent.
- **Children's Online Privacy Protection Act (1998)**
- According to the Children's Online Privacy Protection Act (COPPA), any website that caters (provide people with things they need) 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 (spread (something, especially information) widely) 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.

- Hasbro, Mattel, Viacom, and JumpStart Games were fined a total of $835,000 in 2016 for violation of the COPPA in connection with technology used by these companies that allowed third-party marketing and advertising companies to use cookies and IP addresses to gain access to the personal information of children under 13 years old without getting their parents' approval first.
- The companies were also forced to change their systems to protect the information of child users from being tracked.

- **Electronic Surveillance**
- This section discusses 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 against Americans at home and abroad.
- The net result is that the scope of government surveillance has greatly expanded—going from collecting data on as few people as necessary to collecting data on as many people as possible.

- 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 (including political activists on both ends of the political spectrum) 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.

- **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 [to believe] 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.”
- Title III court orders must describe the duration and scope of the surveillance, the conversations that may be captured, and the efforts to be taken to avoid capture of innocent conversations.

- **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.
- The FISA court must be satisfied, based on a probable cause standard, that the U.S. person is an agent of a foreign power or an officer or employee of a foreign power.
- FISA also created the FISA Court, which meets in secret to hear applications for orders approving electronic surveillance anywhere within the United States.

- **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.

- 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.

- **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 dialing, routing, addressing, and signaling information without a search warrant.
- ECPA was passed as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act.

- 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.

General Data Protection Regulation (GDPR)

- The General Data Protection Regulation 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.

- 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 (hiding) the existence of any personal data record-keeping systems.
- **Freedom of Information Act**
- 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 (unwilling) 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.

KEY PRIVACY AND ANONYMITY ISSUES

- The rest of this chapter discusses a number of current and important privacy issues, including 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 analyze browsing habits and deduce personal interests and preferences.
- The use of cookies and tracking software is controversial because companies can collect information about consumers without their explicit permission.
- 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.

- Marketing firms aggregate the information they gather about consumers to build databases that contain a huge amount of consumer data.
- They want to know as much as possible about consumers—who they are, what they like, how they behave, and what motivates them to buy.
- The marketing firms provide these data to companies so that they can tailor their products and services to individual consumer preferences.
- Advertisers use the data to more effectively target and attract customers to their messages.

- 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 (originating) from privacy violations.
- A **data breach** is the unintended release of sensitive data or the access of sensitive data (e.g., credit card numbers, health insurance member ids, and Social Security numbers) by unauthorized individuals.

TABLE 4-4 Largest data breaches in the past five years

Organization	Year breach occurred	Number of records compromised	Data stolen
Yahoo	2013	1 billion	Usernames, passwords, email addresses, and security questions and answers
Yahoo	2014	500 million	Real names, dates of birth, email addresses, and telephone numbers
FriendFinder	2016	412 million	Usernames, passwords, and email addresses
LinkedIn	2012	165 million	Email addresses and passwords
Target	2013	110 million	Real names, addresses, email addresses, telephone numbers, and credit and debit card data

- **Identity theft** is the theft of personal information, which is then used without the owner's permission.
- Often, stolen personal identification information, such as a person's name, Social Security number, or credit card number, is used to commit fraud or other crimes.
- Thieves may use a consumer's credit card number to charge items to that person's account, use identification information to apply for a new credit card or a loan in a consumer's name, or use a consumer's name and Social Security number to obtain government benefits.
- Thieves also often sell personal identification information on the black market.

- **Electronic Discovery**
- 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.

- **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.

- 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.
- A key issue is the scope of e-discovery (e.g., how many years of ESI will be requested and what topics and/or individuals need to be included in the e-discovery process).

- Often organizations will send a litigation (the process of taking legal action) 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.
- 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.
- Traditional software development firms as well as legal organizations have recognized the growing need for improved processes to speed up and reduce the costs associated with e-discovery.
- As a result, dozens of companies now offer e-discovery software that provides the ability to do the following:
  - Analyze large volumes of ESI quickly to perform early case assessments
  - Simplify and streamline data collection from across all relevant data sources in multiple data formats

- Cull (Choose) large amounts of ESI to reduce the number of documents that must be processed and reviewed
- Identify all participants in an investigation to determine who knew what and when

- Predictive coding is a process that couples human guidance with computer-driven concept searching in order to “train” document review software to recognize relevant documents within a document universe.
- It is used to reduce a large set of miscellaneous documents that may or may not be of interest to a much smaller set of documents (5 to 20 percent of the original set) that are pertinent (relevant) to a legal case or FOIA inquiry.

- Predictive coding greatly accelerates the actual review process while also improving its accuracy and reducing the risk of missing key documents.
- Two key issues are raised with the use of predictive coding:
  - (1) are attorneys still able to meet their legal obligations to conduct a reasonable search for pertinent documents using predictive coding and
  - (2) how can counsel safeguard a client's attorney-client privilege if a privileged document is uncovered?

- E-discovery raises many ethical issues:
  - Should an organization ever attempt to destroy or conceal incriminating evidence that could otherwise be revealed during discovery?
  - To what degree must an organization be proactive and thorough in providing evidence sought through the discovery process?
  - Should an organization attempt to bury incriminating evidence in a mountain of trivial, routine ESI?

- **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.

- Your employer may legally monitor your use of any employer-provided mobile phone or computing device including contact lists, call logs, email, location, photos, videos, and web browsing.
- Many employers permit their employees to use their own personal mobile phones or computing devices for work purposes in a policy called Bring Your Own Device (BYOD).
- Such a policy should spell out the degree to which use of such devices may be monitored.
- Many companies encourage their employees to wear fitness trackers as part of an organizational fitness program.

- Devices from Apple, Fitbit, and others collect valuable data on employee's health and physical movement but can also open the door to numerous ethical and legal issues.
- For example, suppose a production floor worker's tracking device reveals the worker is less mobile and active than his peers.
  - Can the employer use this data to justify firing the employee or moving him to another position?
  - Should the employer investigate whether the data indicate the worker has a physical disability that requires the employer to make a reasonable accommodation?
  - If the employer takes no action, can the employer be sued for failure to provide a reasonable accommodation in light of evidence the worker had a disability?

- Society is still struggling to define the extent to which employers should be able to monitor the work-related activities of employees.
- On the one hand, employers want to be able to guarantee a work environment that is conducive to all workers, ensure a high level of worker productivity, and limit the costs of defending against privacy-violation lawsuits filed by disgruntled employees.
- On the other hand, privacy advocates want federal legislation that keeps employers from infringing on the privacy rights of employees.
- Such legislation would require prior notification to all employees of the existence and location of all electronic monitoring devices.

- Privacy advocates also want restrictions on the types of information collected and the extent to which an employer may use electronic monitoring.
- As a result, privacy bills are being introduced and debated at the state and federal levels.
- As the laws governing employee privacy and monitoring continue to evolve, business managers must stay informed in order to avoid enforcing outdated usage policies.
- Organizations with global operations face an even greater challenge because the legislative bodies of other countries also debate these issues.

- **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 (critical observation or examination) 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 (based on personal experiences, not official information) data that suggest the cameras are effective in preventing crime and terrorism.
- They can provide examples in which cameras helped solve crimes by corroborating (confirm or give support to) the testimony of witnesses and helping to trace suspects.

- There are 5.9 million closed circuit TV cameras (CCTV) in operation throughout Great Britain—which amounts to 1 CCTV camera for every 10 people.
- **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.

- 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.
- 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.

- The fact that most cars now come equipped with an EDR and that the data from this device may be used as evidence in a court of law is not broadly known by the public.
- The future capabilities of EDRs and the extent of use of their data in court proceedings remain to be seen.
- **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.
- 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.

- There is no law that prohibits a business from making an app whose primary purpose is to help one person track another, and anyone can purchase this type of software over the Internet.
- However, it is illegal to install the software on a phone without the permission of the phone owner.
- It is also illegal to listen to someone's phone calls without their knowledge and permission.
- However, these legal technicalities are not a deterrent for a determined stalker.

FIRST AMENDMENT RIGHTS

- The Internet enables a worldwide exchange of news, ideas, opinions, rumors, 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 (attempt to find something) to conserve corporate network capacity, avoid legal liability, and improve worker productivity by limiting the nonbusiness use of IT resources.
- 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 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 nonverbal, 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 (encouragement of another person to commit a crime) of panic, incitement to crime, “fighting words,” and sedition.
- 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 (offensive or taboo) 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?

- These three tests have become the U.S. standard for determining whether something is obscene.
- The requirement that a work be assessed by its impact on an average adult in a community has raised many questions:
  - Who is an average adult?
  - What are contemporary community standards?
  - What is a community? (This question is particularly relevant in cases in which potentially obscene material is displayed worldwide via the Internet.)

- **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.

- A woman sued Gawker Media (a controversial, now-defunct, website that trafficked in news, gossip, and opinion) and its founder for defamation and invasion of privacy.
- She claimed that a Gawker's blog post speculating that she was dating her boss at tech company Yahoo damaged her reputation and caused her to suffer personally and professionally by stating that she did not conduct herself professionally and ethically and exercised poor judgment in her senior position in the firm's human resources organization.

FREEDOM OF EXPRESSION: 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.
- This section discusses a number of key issues related to the freedom of expression, including controlling access to information on the Internet, Internet censorship, SLAPP lawsuits, anonymity on the Internet, John Doe lawsuits, hate speech, pornography on the Internet, and fake news reporting.

- **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.

- **Communications Decency Act**
- The Telecommunications Act 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.

- **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.

- **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.

- **Internet Censorship**
- Internet censorship is the control or suppression of the publishing or accessing of information on the Internet.
- Speech on the Internet requires a series of intermediaries to reach its audience 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.

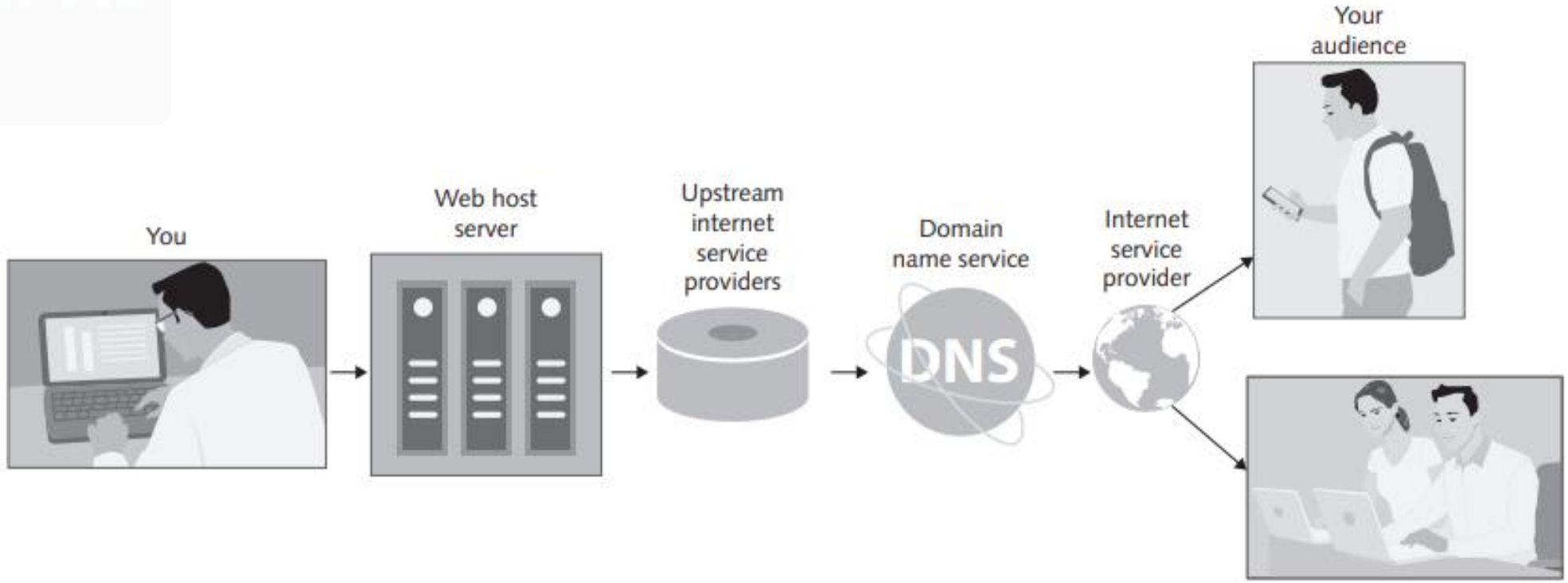

FIGURE 5-3 Internet Censorship

- **Strategic Lawsuit Against Public Participation**
- 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.

- **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.
- **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.
- **Doxing** involves doing research on the Internet to obtain someone's private personal information—such as home address, email address, phone numbers, and place of employment —and even private electronic documents, such as photographs, and then posting that information online without permission.
- Doxing may be done as an act of revenge for a perceived slight or as an effort to publicly shame someone who has been operating anonymously online. Sadly, in some cases it is simply done for kicks.

- Maintaining anonymity on the Internet is important to some computer users.
- They might be seeking help in an online support group, reporting defects about a manufacturer’s goods or services, taking part in frank discussions of sensitive topics, expressing a minority or antigovernment opinion in a hostile political environment, or participating in chat rooms.
- Other Internet users, however, would prefer to ban web anonymity because they think its use increases the risks of defamation and fraud, as well as the exploitation of children.

- **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.

- **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.
- **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 nontraditional sources—some of which offer more objective, verifiable news reporting than others—including the following types: Blogs, Fake News Site, Social Media Sites, etc

SOCIAL NETWORKING ETHICAL ISSUES

- When you have an Internet community of nearly 4 billion people online, not everyone is going to be a good “neighbor” and abide by the rules of the community.
- Many will stretch or exceed the bounds of generally accepted behavior.
- 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.
- **Cyberabuse, Cyberharassment, and Cyberstalking**
- 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.
- Instances of cyberabuse are not always clear. 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** is a subcategory of cyberabuse that consists of a long-term pattern of unwanted, persistent pursuit and intrusive behavior (involving the use of an electronic communications device) that is directed by one person against another 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.
- Note that cyberharassment differs from cyberstalking in that it is aimed at tormenting an individual but does not involve a credible threat of physical harm.

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.	

- The National Center for Victims of Crime offers a detailed set of recommended actions to combat cyberstalking, including the following:
  - Contact local law enforcement authorities to obtain a restraining order prohibiting any further contact with you.
  - Inform your ISP provider as well as the stalker's ISP.
  - Provide the stalker a written notice that their contact is unwanted and that all further contact must cease.
  - Consider suspending your social networking accounts until the cyberstalking situation has been resolved.
  - Gather as much physical evidence as possible and document each instance of abusive contact.
  - Never agree to meet with the stalker to "talk things out."

- **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.
- The Sex Offender Registration and Notification Provisions (SORNA) of the Adam Walsh Child Protection and Safety Act of 2006 improved on the Wetterling Act by setting national standards that govern which sex offenders must register and what data must be captured, as shown in Table 9-7.

TABLE 9-7 Sex offender SORNA data requirements

Data provided by the sex offender	Data provided by jurisdiction in which the offender is registered
• Name • Social Security number • Residence address • Name and address of place of employment • Name and address of any school attending • License plate and description of any auto owned or operated by the offender	• Physical description of the sex offender • Text defining the sex crime for which the offender is registered • Criminal history of the offender including the date of all arrests and convictions • A current photo of the offender • A copy of the driver's license or photo ID issued to the offender by the jurisdiction • A set of fingerprints and palm prints • A DNA sample

- **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 nonconsensual 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.
- 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.
- Many examples of an effective employee social media policy that can be customized to meet your company's specific needs can be found online.

- **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 Chapter 3