Chapter 3
Privacy and Freedom of Expression

Privacy Protection and The Law

- Government and businesses use IT systems to gather, store, analyze, and report information about people to make better decisions; The different information gathered is: sexual orientation, web browsing behavior, associations and affiliations, driving record, educational records, financial data, location data, medical history, police record, work history etc.
- However, many people object to the data collection policies of governments and businesses; For these people, the existing privacy laws and practices fails to provide adequate protection to their privacy

Privacy Protection and The Law

- 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 privacy
  - Appropriate corporate policies must be developed to set baseline standards for people's privacy
  - Education and communication are also essential
- Few laws provide privacy protection, and most people assume that they have greater privacy rights than the law actually provides

Privacy Protection and The Law

- **Information Privacy:**
  - **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”
  - **Information Privacy:** Information privacy is the impact of IT on privacy
    - 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 Protection and The Law

- **Privacy Laws, Applications, and Court Rulings:**
  - Different legislative acts have been exercised by governments around the world to address invasion of privacy
  - 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 national data privacy policy has been developed
  - 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

Privacy Protection and The Law

- **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 such as credit cards, loans, brokerage accounts etc.
  - 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 and whether or not they are shared with other people or companies
  - Some acts related with financial data are **Fair Credit Reporting Act (1970)**, **Right to Financial Privacy Act (1978)**, **Gramm-Leach-Bliley Act (1999)** and **Fair and Accurate Credit Transactions Act (2003)**

Privacy Protection and The Law

- The **Fair Credit Reporting Act** regulates the operations of credit reporting bureaus, including how they collect, store, and use credit information
- The **Right to Financial Privacy Act** protects the records of financial institution customers from unauthorized scrutiny by the federal government; 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
- The **Gramm-Leach-Bliley Act**, was a bank deregulation law that enabled institutions to offer investment, commercial banking, and insurance services; Before that, individual companies were only allowed to offer one of those types of financial service products; This act also included three key rules that affect personal privacy

Privacy Protection and The Law

- The **Fair and Accurate Credit Transactions Act** is 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

Privacy Protection and The Law

- **Health Information:**
  - The electronic medical records concerning health of individuals should be protected
  - 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; Healthcare providers must obtain written consent from patients prior to disclosing any information from their medical records
  - The **American Recovery and Reinvestment Act** includes strong privacy provisions for electronic health records (EHRs); It also mandated that each individual whose health information has been exposed be notified within 60 days after discovery of a data breach

Privacy Protection and The Law

- **Children's Personal Data:**
  - A recent survey revealed that children spend more hours watching television, playing video games, social networking, browsing websites, or doing other things on a computer, smartphone, or tablet; Children should be protected from inappropriate behavior
  - **Family Education Rights and Privacy Act (1974)** assigns rights to parents regarding their children's education records; Rights transfer to student once student becomes 18
  - According to **Children's Online Privacy Protection Act (1998)** any web site that caters to children must offer comprehensive privacy policies, notify parents or guardians about its data-collection practices, and receive parental consent before collecting personal information from children under 13

Privacy Protection and The Law

- **Electronic Surveillance:**
  - In recent years, new laws addressing government surveillance have been added and old laws amended in reaction to the development of new communication technologies
  - **Title III of the Omnibus Crime Control and Safe Streets Act (1968; amended 1986)**, 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

Privacy Protection and The Law

- **Foreign Intelligence Surveillance Act (1978)** 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
- **Executive Order 12333 (1981)** 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

Privacy Protection and The Law

- **Electronic Communications Privacy Act (1986)** 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
- **Communications Assistance for Law Enforcement Act (1994)** requires 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
- **USA PATRIOT Act (2001)** increased ability of law enforcement agencies to search telephone, email, medical, financial, and other records

Privacy Protection and The Law

- **Fair Information Practices:**
  - Fair information practices is a term for a set of guidelines that govern the collection and use of personal data; The overall goal 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
  - **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 consisting of more than 30 member countries; The OECD's fair information practices, established in 1980, are often held up as the model for ethical treatment of consumer data

Privacy Protection and The Law

- **European Union Data Protection Directive (1995)** requires any company doing business within EU countries 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
- **European-United States Privacy Shield Data Transfer Program Guidelines** places stronger obligations on companies in the United States to protect the personal data of Europeans and requires stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission

Privacy Protection and The Law

- **General Data Protection Regulation (GDPR)** 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

Privacy Protection and The Law

- **Access to Government Records:**
  - The U.S. government has a great capacity to store data about each and every one and about the proceedings of its various agencies
  - **Freedom of Information Act (1966; amended 1974)** grants journalists and citizens the right to access certain information and records of federal, state, and local governments upon request that the government is reluctant to release
  - **Privacy Act (1974)** prohibits government agencies from concealing the existence of any personal data record-keeping system; Outlines 12 requirements that each record-keeping agency must meet; Central Intelligence Agency and law enforcement agencies are excluded from this act; Does not cover actions of private industry

Key Privacy and Anonymity Issue

- Some current and important privacy issues are *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

Key Privacy and Anonymity Issue

- 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 as companies can collect information about consumers without their explicit permission
- Similar controversial methods are used outside the Web environment
- Marketing firms aggregate the information they gather about consumers to build databases that contain a huge amount of consumer data; The marketing firms provide these data to companies so that they can tailor their products and services to individual consumer preferences

Key Privacy and Anonymity Issue

- After the data have been collected, consumers have no way of knowing how it is used or who is using it
- 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; 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
- **Identity theft** is the theft of personal information, which is then used without the owner's permission to commit fraud or other crimes

Key Privacy and Anonymity Issue

- **Electronic Discovery (e-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, photographs, files, sound recordings etc. stored on any form of storage device
  - Through the e-discovery process, it is quite likely that various forms of ESI of a private or personal nature will be disclosed
  - Federal Rules of Procedure define e-discovery processes

Key Privacy and Anonymity Issue

- Often organizations will send a **litigation hold notice** (document preservation notice) that informs to save relevant data and to suspend data that might be due to be destroyed based on normal data-retention rules
- E-discovery is complicated and requires extensive time to collect, prepare, and review data
- 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 large amounts of ESI to reduce the number of documents that must be processed and reviewed

Key Privacy and Anonymity Issue

- 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

– 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

Key Privacy and Anonymity Issue

- **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
  - 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
  - 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

Key Privacy and Anonymity Issue

- 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; 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
- Public-sector employees have far greater privacy rights than in the private industry

Key Privacy and Anonymity Issue

- **Advanced Surveillance Technology:**
  - Surveillance cameras and satellite-based systems can pinpoint a person's physical location providing amazing new data-gathering capabilities
  - These advances can also diminish individual privacy and complicate the issue of how much information should be captured about people's private lives
  - Advocates of advanced surveillance technology argue that people have no legitimate expectation of privacy in a public place and thus privacy rights do not apply
  - Critics raise concerns about the use of surveillance to secretly store images of people, creating a new potential for abuse, raise the possibility that such technology may not identify people accurately

Key Privacy and Anonymity Issue

- **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 argue that cameras are effective in preventing crime and terrorism
- **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

Key Privacy and Anonymity Issue

- 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

Key Privacy and Anonymity Issue

- **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
  - Information gathered can be sent to the user's email account to be accessed live or at a later time

Key Privacy and Anonymity Issue

- 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

- First amendment to U.S. Constitution protects rights to freedom of religion, freedom of expression, and freedom to assemble peaceably
- 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
  - Sedition

First Amendment Rights

- **Obscene Speech:**
  - 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

First Amendment Rights

- **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

Freedom of Expression: Key Issues

- There are 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:**
  - Freedom of speech on the Internet is complicated by ease by which children can access Internet because it is difficult to restrict their access without also restricting adults' access
  - This issue has been addressed by laws and special software to block access to objectionable material

Freedom of Expression: Key Issues

- **Communications Decency Act (CDA):**
  - This act 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 (COPA) :**
  - 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”

Freedom of Expression: Key Issues

- **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
  - URL filtering does not allow to access a particular URL or domain name belonging to an objectionable site
  - Keyword filtering uses keywords or phrases – such as sex, Satan, and gambling – to block websites
  - Dynamic content filtering evaluates each website's content immediately before it is displayed using object analysis and image recognition techniques

Freedom of Expression: Key Issues

- The negative side of filtering 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 with objectionable material; The use of filters can also ensure that employees do not waste their time viewing nonbusiness-related websites
- Some internet filters for home users include Net Nanny, SpyAgent, and Qustodio; Internet software filters have also been developed to run on mobile devices
- Another approach to restricting access to websites is to subscribe to an ISP that performs the blocking; The blocking occurs through the ISP's server rather than via software loaded onto each user's computer

Freedom of Expression: Key Issues

- **Children's Internet Protection Act (CIPA):**
  - 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
  - Any school or library that failed to comply with the law would no longer be eligible to receive federal money
  - Implementing CIPA in libraries is much more difficult because a library's services are open to people of all ages, including adults who have First Amendment rights to access a broader range of online materials than are allowed under CIPA

Freedom of Expression: Key Issues

- **Digital Millennium Copyright Act (DMCA):**
  - DMCA addresses a number of copyright-related issues
  - The DMCA is divided into five titles and 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
  - 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

Freedom of Expression: Key Issues

- **Internet Censorship:**
  - Internet censorship is the control or suppression of publishing or accessing of information on the Internet
  - 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 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

Freedom of Expression: Key Issues

- Several countries have enacted 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 where authorities have control over DNS servers and 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
- Internet censorship in China is perhaps the most rigorous in the world; The Chinese government blocks access to websites that are considered objectionable

Freedom of Expression: Key Issues

- **Strategic Lawsuit Against Public Participation (SLAPP):**
  - A SLAPP is employed by corporations, government officials, and others against citizens and community groups who oppose them on matters of public interest
  - Many people question the ethics and legality of using a SLAPP; others claim that all is fair when it comes to politics and political issues
  - Every year thousands of people become SLAPP victims while participating in perfectly legal actions such as phoning a public official, speaking out at a public meeting, or circulating a petition etc.
  - Anti-SLAPP laws are designed to reduce frivolous SLAPPs

Freedom of Expression: Key Issues

- **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
  - Maintaining anonymity on the Internet is important to some computer users; Other Internet users, however, would prefer to ban web anonymity because they think its use increases the risks

Freedom of Expression: Key Issues

- **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

Freedom of Expression: Key Issues

- 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)
- ISPs and social networking sites receive more than a thousand subpoenas per year directing them to reveal the identity of John Does

Freedom of Expression: Key Issues

- **Hate Speech:**
  - Hate speech is spoken words or writing that are offensive, insulting, and/or threatening to an individual or group based on a particular attribute; Targeted attributes are ethnic background, sexual orientation, race, or disability etc.
  - 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 hate speech
  - ISPs and social networking sites do reserve the right to remove content that, in their judgment, does not meet their standards

Freedom of Expression: Key Issues

- **Pornography on the Internet:**
  - Many people, including some free-speech advocates, believe that there is nothing illegal or wrong about purchasing adult pornographic material
  - On the other hand, most parents, educators, and other child advocates are concerned that children might be exposed to online pornography
  - Internet has been a boon to the pornography industry by providing fast, cheap, and convenient access to many millions of porn websites worldwide
  - If what someone distributes or exhibits is judged obscene, they are subject to prosecution under the obscenity laws

Freedom of Expression: Key Issues

- Many companies believe that they have a duty to stop the viewing of pornography in the workplace; Reasonable steps include:
  - Establishing and communicating an acceptable use policy that prohibits access to pornography sites
  - Identifying those who violate the policy
  - Taking disciplinary action against those who violate the policy, up to and including termination
- Few companies take opposite viewpoint; They believe the best approach is to ignore the problem by never investigating it; Many people would consider such approach unethical and would view management as shirking an important responsibility to provide a work environment free of sexual harassment

Freedom of Expression: Key Issues

- 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
- **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
- The **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** specifies requirements that commercial emailers must follow when sending messages that have a primary purpose to advertise or promote a commercial product or service

Freedom of Expression: Key Issues

- **Fake News:**
  - Much online news continues to come from traditional news sources; However, readers looking for news and information online will also find a wide range of nontraditional online sources including **blogs**, **fake news sites**, and **social media sites**
  - Bloggers may be less likely to remain unbiased, instead stating their opinion and supporting facts without presenting the other side of an argument
  - Fake news 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

Freedom of Expression: Key Issues

- Social media sites 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

Social Networking Ethical Issues

- Not everyone in the social media 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 are online abuse, harassment, stalking, cyberbullying, encounters with sexual predators, the uploading of inappropriate material, and the participation of employees in social networking
- Other issues include increased risk of accidents with social media interaction while driving, the tendency to become narcissist in their postings, and the ability to perform self-image manipulation

Social Networking Ethical Issues

- **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
  - Cyberabuse encompasses both **cyberharassment** and **cyberstalking**
  - **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

Social Networking Ethical Issues

- **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
  - 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
  - Cyberstalking includes abusive or excessive phone calls, threatening or obscene mail, trespassing, vandalism, physical stalking, and even physical assault

Social Networking Ethical Issues

- **Encounters with Sexual Predators:**
  - Some social networking platforms have been criticized for not doing enough to protect minors from encounters with sexual predators
  - Legislators are pushing social networking Web sites to adopt stronger safety measures
- **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

Social Networking Ethical Issues

- The policies set specific limits on content that is sexually explicit, defamatory, hateful, violent, or that promotes illegal activity
- Most Web sites do not have sufficient resources to review all material posted

- **Employee Participation on Social Media Networks:**
  - 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