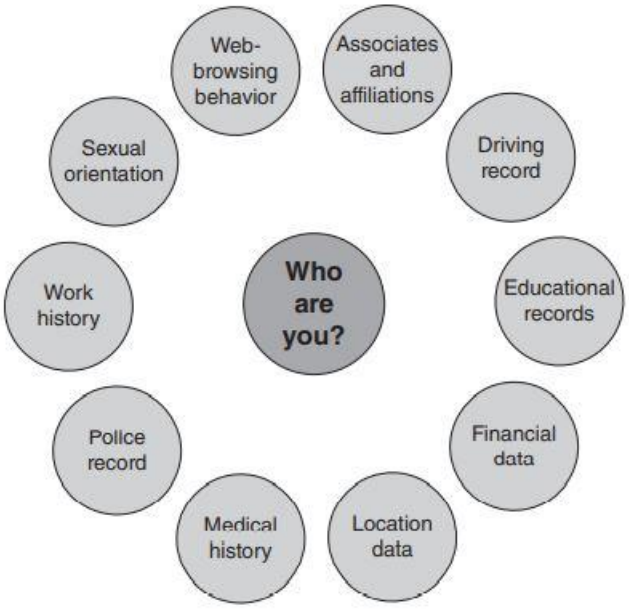
# Unit 3: Privacy and Freedom of Expression

**Contents:**



## 3.1 Privacy Protection and the Law – Information Privacy, Privacy Laws, Applications, and Court Rulings

The use of information technology in both government and non-government sector 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 extremely 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.

However, many people object to the data collection policies of governments and businesses on the grounds that they strip individuals of the power to control their own personal information.

For these people, the existing hodgepodge of privacy laws and practices fails to provide adequate protection; rather, it causes confusion that promotes doubt and disbelief, 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.

Today, in addition to protection from government intrusion, people want and need privacy protection from private industry. Few laws provide such protection, and most people assume that they have greater privacy rights than the law actually provides.

Some people believe that only those with something to hide should be concerned about the loss of privacy; however, others believe that everyone should be concerned.

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

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 approved and became known as the Bill of Rights. So, although the Constitution does not contain the word privacy, the U.S. Supreme Court has ruled that the concept of privacy is protected by the Bill of Rights.

The Constitution of Nepal-2072

Part-3 Fundamental Rights and Duties [ मौलिक हक र कर्तव्य ]

28. Right to privacy: The privacy of any person, his or her residence, property, document, data, correspondence and matters relating to his or her character shall, except in accordance with law, be inviolable.

२८ गोपनीयताको हक : कुनै पनि व्यक्तिको जीउ, आवास, सम्पत्ति, लिखत, तथ्यांक, पत्राचार र चरित्र सम्बन्धी विषयको गोपनीयता कानून बमोजिम बाहेक अनतिक्रम्य हुनेछ ।

The Privacy Act, 2075 (2018)

The act contains provisions related to privacy of

- Body and Family of Person
- Relating to Residence
- Relating to Property
- Relating to Document
- Relating to Data

- Relating to Correspondence
- Relating to Character
- Electronic Means and Privacy
- Collection and Protection of Personal Information
- Offences and Punishment
- Miscellaneous

ETA-2063 contains a provision related to privacy:

48. Confidentiality to Divulge: Save otherwise provided for in this Act or Rules framed hereunder or for in the prevailing law, if any person who has an access in any record, book, register, correspondence, information, documents or any other material under the authority conferred under this Act or Rules framed hereunder divulges or causes to divulge confidentiality of such record, books, registers, correspondence, information, documents or materials to any unauthorized person, he/she shall be liable to the punishment with a fine not exceeding Ten Thousands Rupees or with imprisonment not exceeding two years or with both, depending on the degree of the offence.

४८. गोपनीयता भङ्ग गर्ने : यो ऐन वा यस ऐन अन्तर्गत बनेका नियमहरु वा प्रचलित कानूनमा अन्यथा व्यवस्था भएकोमा बाहेक यो ऐन वा यस ऐन अन्तर्गत बनेका नियमहरु अन्तर्गत प्रदान गरिएको कुनै अधिकार बमोजिम कुनै विद्युतीय अभिलेख, किताब, रजिष्टर, पत्रव्यवहार, सूचना, कागजात वा अन्य सामग्रीहरुमा पहुँच प्राप्त गरेको कुनै व्यक्तिले कुनै अनधिकृत व्यक्तिलाई त्यस्तो अभिलेख, किताब, रजिष्टर, पत्र व्यवहार, सूचना, कागजात वा सामग्रीको गोपनीयता भङ्ग गरेमा वा भङ्ग गर्न लगाएमा निजलाई कसूरको मात्रा हेरी एक लाख रुपैयाँसम्म जरिबाना वा दुई वर्षसम्म कैद वा दुवै सजाय हुनेछ ।

**Information Privacy**

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

Another concept of privacy that is particularly useful in discussing the impact of IT on privacy is the term information privacy, first coined by Roger Clarke, director of the Australian Privacy Foundation. Information privacy is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one’s personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and their use).

**Privacy Laws, Applications, and Court Rulings**

In this section we will study legislative acts that affect a person’s 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, primary 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.

Privacy laws generally includes topics like: financial data, health information, children’s personal data, electronic surveillance, fair information practices, and access to government records.

The constitution of Nepal includes Right to Privacy as one of the Fundamental Rights and Duties. In the context of this Rights, the Privacy Act 2075 enacted to provide legal provisions.

The Privacy Act, 2075 (2018)

**Preamble:**

Whereas, it is expedient to make legal provisions on promoting dignified living standards by making provisions to ensure the right to privacy of the matters relating to body, residence, property, document, data, correspondence and character of every person, to manage the protection and safe use of personal information remained in any public body or institution, and to prevent encroachment on the privacy of every person; Now, therefore be it enacted by the Federal Parliament.

**Chapter 1: Preliminary [ प्रारम्भिक ]**

1. Short title and commencement: (1) This Act may be cited as the “Privacy Act, 2075 (2018)."

(2) This Act shall come into force immediately.

2. Definitions:

(c) "Personal information" means the following information related to any person:

(1) His or her caste, ethnicity, birth, origin, religion, color or marital status,

(2) His or her education or academic qualification,

(3) His or her address, telephone or address of electronic letter (email)

(4) His or her passport, citizenship certificate, national identity card number, driving license, voter identity card or details of identity card issued by a public body,

(5) A letter sent or received by him or her to or from anybody mentioning personal information,

(6) His or her thumb impressions, fingerprints, retina of eye, blood group or other biometric information,

(7) His or her criminal background or description of the sentence imposed on him or her for a criminal offence or service of the sentence,

(8) Matter as to what opinion or view has been expressed by a person who gives professional or expert opinion, in the process of any decision.

**Chapter 2: Privacy of Body and Family of Person [ व्यक्तिको जीउ तथा पारिवारिक गोपनीयता ]**

3. Privacy of body and personal life of person [ व्यक्तिको शारीरिक तथा निजी जीवनको गोपनीयता ]

4. To have family privacy [ पारिवारिक गोपनीयता हुने ]

5. Not to search body [ शरीरको तलासी लिन नहुने ]

6. Privacy relating to reproductive health and pregnancy: [ प्रजनन स्वास्थ्य र गर्भावस्था सम्बन्धी गोपनीयता ]

**Chapter 3: Privacy Relating to Residence [ आवास सम्बन्धी गोपनीयता ]**

7**.** To have privacy of residence [ आवासको गोपनीयता हुने ]

8. To provide notice while entering into residence [ आवासमा प्रवेश गर्दा सूचना दिनु पर्ने ]

9. Not to install CCTV camera in the residence [ आवासमा सिसिटिभि क्यामेरा जडान गर्न नहुने ]

**Chapter 4: Privacy Relating to Property [ सम्पत्ति सम्बन्धी गोपनीयता ]**

10. To have privacy of property [ सम्पत्तिको गोपनीयता हने ]

**Chapter 5: Privacy Relating to Document [ लिखत सम्बन्धी गोपनीयता ]**

11. To have privacy of document [ लिखत गोपनीयता हुने ]

**Chapter 6: Privacy Relating to Data [ तथ्याङ्क सम्बन्धी गोपनीयता ]**

12. To have privacy of data [ तथ्याङ्कको गोपनीयता हुने ]

**Chapter 7: Privacy Relating to Correspondence []**

13. To have privacy of correspondence [ पत्राचारको गो **पत्राचार सम्बन्धी गोपनीयता** पनीयता हुने ]

14. Not to open letters [ चिट्ठीपत्र खोल्न नहुने ]

**Chapter 8: Privacy Relating to Character [ चरित्र सम्बन्धी गोपनीयता ]**

15. To have privacy of character [ चरित्रको गोपनीयता हुने ]

16. Not to take or sell photograph [ तश्विर खिच्न वा बिक्री गर्न नहुने ]

17. Not to make the person under investigation public [ अनसुन्धानको सिलसिलामा रहेको व्यक्तिलाई सार्वजनिक गर्न नहुने]

18. Not to disclose confidential matter [ गोप्य कुरा प्रकट गर्न नहुने ]

**Chapter 9: Electronic Means and Privacy [ विद्युतीय माध्यम र गोपनीयता ]**

19. To have privacy of electronic means [ विद्युतीय माध्यमको गोपनीयता हुने ]

20. Relating to installing CCTV camera at public place [ सार्वजनिक स्थलमा सिसिटिभि क्यामेरा जडान गर्ने सम्वन्धमा]

21. Not to make surveillance or espionage [ निगरानी वा जासुसी गर्न नहुने ]

22. Not to use drone [ ड्रोन प्रयोग गर्न नहुने ]

**Chapter 10: Collection and Protection of Personal Information [ वैयक्तिक सूचना सङ्कलन तथा संरक्षण ]**

23. Not to collect personal information except in accordance with law [कानून बमोजिम बाहेक वैयक्तिक सूचना सङ्कलन गर्न नहुने]

24. Not to deem to be personal information [वैयक्तिक सूचना नमानिने]

25. Protection of collected information [सङ्कलित सूचनाको संरक्षण]

26. Not to use personal information without consent [सहमतिविना वैयक्तिक सूचनाको उपयोग गर्न नहुने]

27. Not to process sensitive information [संवेदनशील सूचना प्रशोधन गर्न नहुने]

28. Application may be made to correct information [सूचना सच्याउन निवेदन दिन सकिने]

**Chapter 11: Offences and Punishment [ कसूर तथा सजाय ]**

29. Offence and punishment [कसूर तथा सजाय]

30. Complaint may be made [उजूर गर्न सक्ने]

31. Compensation [क्षतिपूर्ति]

32. To award departmental punishment [विभागीय सजाय हुने]

**Chapter 12: Miscellaneous [ विविध ]**

33. To obtain consent of guardian or curator [संरक्षक वा माथवर व्यक्तिको मञ्जुरी लिनु पर्ने]

34. Not to deem to be a bar [बाधा पर्याएको नमानिने]

35. Not to act contrary to this Act [यस ऐन प्रुतिकूल गर्न नहुने]

36. Power to frame Rules [नियम बनाउने अधिकार]

**Annapurna Rana Case and Court Rulings** [related to privacy act]

[Court decision attached]

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

- The right of privacy is "the right to be left alone—the most comprehensive of rights, and the right most valued by a free people."
- Information privacy is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one's personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use).
- The use of information technology in business requires balancing the needs of those who use the information that is collected against the rights and desires of the people whose information is being used. A combination of approaches—new laws, technical solutions, and privacy policies—is required to balance the scales.
- The Fourth Amendment reads, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The courts have ruled that without a reasonable expectation of privacy, there is no privacy right to protect.
- Today, in addition to protection from government intrusion, people want and need privacy protection from private industry. For many, the existing hodgepodge of privacy laws and practices fails to provide adequate protection and fuels a sense of distrust and skepticism, and concerns over identity theft.

## **3.2 Key Privacy and Anonymity Issues** – Consumer profiling, Electronic Discovery, Workplace Monitoring, Surveillance

### **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. 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. Companies that can't protect or don't respect customer information often lose business, and some become offenders 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. The cost to an organization that suffers a data breach can be quite high—by some estimates nearly $200 for each record lost. Nearly half the cost is typically a result of lost business opportunity associated with the customers whose patronage has been lost due to the incident. Other costs include public relations–related costs to manage the firm's reputation, and increased customer-support costs for information hotlines and credit monitoring services for victims. Largest U.S. 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.

Organizations are often reluctant to announce data breaches due to the ensuing bad publicity and potential for lawsuits by angry customers. However, victims whose personal data were compromised during a data breach need to be informed so that they can take protective measures. Publicly traded organizations have an obligation to report significant data breaches to concerned authorities. Most states have laws that require businesses to notify the state and/or affected consumers in a timely fashion of data breaches that compromise more than a set amount of consumer data. About 300 publicly listed U.S. companies reported cybersecurity incidents to a state regulator or directly to affected consumers over the past six years, although not all were reported in a timely fashion.

For example, the New York attorney general imposed a fine of $50,000 for delays in the reporting of two data breaches involving some 70,000 credit card numbers and other personal data at the Trump Hotels chain. As part of the settlement, Trump Hotels was also required to undertake additional security measures, including conducting annual employee security training, performing regular software security testing, and ensuring that contracted service providers implement and maintain appropriate safeguards.

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

- Companies use many different methods to collect personal data about visitors to their websites, including depositing cookies on visitors' hard drives.
- Consumer data privacy has become a major marketing issue—companies that cannot protect or do not respect customer information have lost business and have become defendants in class actions stemming from privacy violations.
- A data breach is the unintended release of sensitive data or the access of sensitive data (e.g., credit card numbers, health insurance member ids, and Social Security numbers) by unauthorized individuals. The increasing number of data breaches is alarming, as is the lack of initiative by some companies in informing the people whose data are stolen. A number of states have passed data breach notifications laws that require companies to notify affected customers on a timely basis.

## Electronic Discovery

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

The Federal Rules of Procedure in US 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 hold notice that informs its employees (or employees or officers of the opposing party) to save relevant data and to suspend data that might be due to be destroyed based on normal data-retention rules.

Apple and Samsung were involved in a dispute involving alleged patent infringement (violation), which led to an additional dispute over litigation hold notices. During the patent infringement litigation (court hearing), the court cited Samsung for failing to circulate a comprehensive litigation hold instruction among its employees when it first anticipated litigation. According to the court, this failure resulted in the loss of emails from several key Samsung employees. Samsung then raised the same issue—Apple had neglected to implement a timely and comprehensive litigation hold to prevent broad destruction of relevant email. A key learning from this case is that an organization should focus on its own ESI preservation and production efforts before it raises issues with its opponent's efforts.

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

discovery can become so expensive and time consuming that some cases are settled just to avoid the costs.

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 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 to a legal case or 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 (advocates) 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?

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

- Discovery is part of the pretrial phase of a lawsuit in which each party can obtain evidence from the other party by various means, including requests for the production of documents.
- E-discovery is the collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings.
- Predictive coding is a process that couples human intelligence with computer-driven concept searching in order to "train" document review software to recognize relevant documents within a document universe

## 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 charge his or her employer for creating an environment favorable 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 disturbing) practices are perfectly legal.

The Fourth Amendment to the Constitution in US protects citizens from unreasonable government searches and is often invoked to protect the privacy of government employees. Public-sector workers can appeal directly to the "reasonable expectation of privacy" standard established by the 1967 Supreme Court ruling in Katz v. United States.

However, the Fourth Amendment cannot be used to limit how a private employer treats its employees. As a result, public-sector employees have far greater privacy rights than those in private industry. Although private-sector employees can seek legal protection against an invasive employer under various state laws, the degree of protection varies widely by state/contries. Furthermore, state privacy laws tend to favor employers over employees. For example, to successfully charge an organization for violation of their privacy rights, employees must prove that they were in a work environment in which they had a reasonable expectation of privacy. As a result, courts typically rule against employees who file privacy claims for being monitored while using company equipment.

A private organization can defeat a privacy claim simply by proving that an employee had been given explicit notice that email, files, and Internet data held on company computers and transferred over company networks were not private and might be monitored.

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 charged 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.

Sapience Analytics offers software that tracks employee activities (e.g., email, texting, calls, analysis, data collection, online meetings, and management activities) and displays them in an app that is visible to both employees and their managers. The tasks are also separated into categories, such as sales or marketing, so that users can see what percentage of their time is spent on the designated core activities and categories for their position.

An IT services company that implemented the software as a "mentoring" tool for its 5,000 employees reported a 90-minute daily increase per person in "core activities" (i.e., coding for a software developer rather than answering emails) after employees were made aware of their work patterns.

**Why and how are employers increasingly using workplace monitoring?**

- Many organizations have developed IT usage policies to protect against employee abuses that can reduce worker productivity and expose employers to harassment lawsuits.
- About 80 percent of U.S. firms record and review employee communications and activities on the job, including phone calls, email, web surfing, and computer files.
- The use of fitness trackers in the workplace has opened up potential new legal and ethical issues.

## 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.

Advocates of advanced surveillance technology argue that people have no legitimate expectation of privacy in a public place. Critics raise concerns about the use of surveillance to secretly store images of people, creating a new potential for abuse, such as intimidation of political rebels or blackmail of people caught with the "wrong" person or in the "wrong" place. Critics also raise the possibility that such technology may not identify people accurately.

**Camera Surveillance**

Surveillance cameras are used in major cities around the world in an effort to discourage crime and terrorist activities. Critics believe that such scrutiny is a violation of civil rights and are concerned about the cost of the equipment and people required to monitor the video feeds. Surveillance camera supporters offer subjective data that suggest the cameras are effective in preventing crime and terrorism. They can provide examples in which cameras helped solve crimes by verifying the evidence 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. China, by way of comparison, has installed 100 million surveillance cameras, or 1 camera for every 14 citizens.

The two most closely monitored cities in the world include Beijing with 477,000 cameras and London with 422,000. The Chicago Transit Authority (CTA) has installed more than 23,000 cameras in an attempt to reduce crime on its rail and bus system. According to the CTA, the cameras helped reduce the overall crime rate on the CTA system by 25 percent from the previous year.

The Domain Awareness system is a joint effort of the New York Police Department and Microsoft to combat terrorist activities and reduce the time required to respond to an incident. The system links together the city's 9,000 surveillance cameras and 600 radiation detectors as well as license plate readers and Police department computer records, including 911 calls. The 40 million dollar system is sensitive enough to tell if a radiation detector was set off by actual radiation, a weapon, or a harmless medical variant. It can also find where a suspect's car is located and track where it has been for the past few weeks. If a suspicious package is left somewhere, police will be able to look back in time and see who left it there. At a press conference announcing the system, New York City mayor dismissed concerns that the system would enable police to achieve "Big Brother" capabilities stating, "What you're seeing is what the private sector has used for a long time. If you walk around with a cell phone, the cell phone company knows where you are.

**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.

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

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

State laws dictate who owns the EDR data, and these provisions vary from state to state. NHTSA must ask permission from the owner of a vehicle before downloading any data for government analysis. Courts can order EDR data for use in court proceedings. There have been numerous cases in which EDR data have been ruled as admissible and reliable in court hearings, and there are cases in which such data have had a significant impact on the findings of the court.

For example, in Howard an accident reconstruction expert was able to use EDR data to determine that the driver was exceeding the speed limit at the time of a fatal accident.

The fact that 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 (Following) 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. (Some users of such software have complained that they contracted malware when downloading stalker apps or that the app failed to work as advertised.) 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 restrictive for a determined stalker.

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

- Surveillance cameras are used in major cities around the world to deter crime and terrorist activities. Critics believe that such security is a violation of civil liberties.
- An EDR is a device that records vehicle and occupant data for a few seconds before, during, and after any vehicle crash that is severe enough to deploy the vehicle's air bags. The fact that most cars now come equipped with an EDR and that the data from this device may be used as evidence in a court of law is not broadly known by the public.

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

## 3.3 First Amendment Rights

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 beliefs 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 peacefully. 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 (untruth), fraud, defamation, obscene speech (offensive), incitement of panic (provocation), incitement to crime, "fighting words," and sedition (incitement of discontent or rebellion against a government).

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

**Obscene Speech**

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

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

1. Would the average person, applying contemporary community standards, find that the work, taken as a whole, appeals to the unhealthy interest?
2. Does the work depict or describe, in a deliberately offensive way, sexual conduct specifically defined by the applicable state law?
3. 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.

**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.

## 3.4 Freedom of Expressions: Key Issues

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

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. Some of these approaches are:

1. Communications Decency Act: It aimed at protecting children from pornography. The CDA imposed $250,000 fines and prison terms of up to two years for the transmission of "indecent" material over the Internet.

   In February 1996, the American Civil Liberties Union (ACLU) and 18 other organizations filed a lawsuit challenging the criminalization of so-called indecency on the web under the CDA. The problem with the CDA was its broad language and vague definition of indecency, a standard that was left to individual communities to determine. In June 1997, the Supreme Court ruled the law unconstitutional and declared that the Internet must be afforded the highest protection available under the First Amendment. The Supreme Court said in its ruling that "the interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of

censorship." The ruling applied essentially the same free-speech protections to communication over the Internet as exist for print communication.

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

Section 230 of the CDA, which was not ruled unconstitutional, states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". This portion of the CDA protects social networking companies such as Facebook and Twitter from defamation suits in connection with user postings that appear on their sites.

2. Child Online Protection Act: In October 1998, the Child Online Protection Act (COPA) was signed into law. 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."

   After its passage, COPA became a rallying point for advocates of free speech. Not only could it affect sellers of explicit material online and their potential customers, but it could ultimately set standards for Internet free speech. Supporters of COPA (primarily the Department of Justice) argued that the act protected children from online pornography while preserving the rights of adults. However, privacy advocacy groups—such as the Electronic Privacy Information Center, the ACLU, and the Electronic Frontier Foundation (EFF)—claimed that the language was overly vague and limited the ability of adults to access material protected under the First Amendment.

   Following a temporary injunction as well as numerous hearings and appeals, in June 2004 the Supreme Court ruled in Ashcroft v. American Civil Liberties Union that there would be "a potential for extraordinary harm and a serious chill upon protected speech" if the law went into effect. The ruling made it clear that COPA was unconstitutional and could not be used to shelter children from online pornography.

**Internet Filtering**

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

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

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

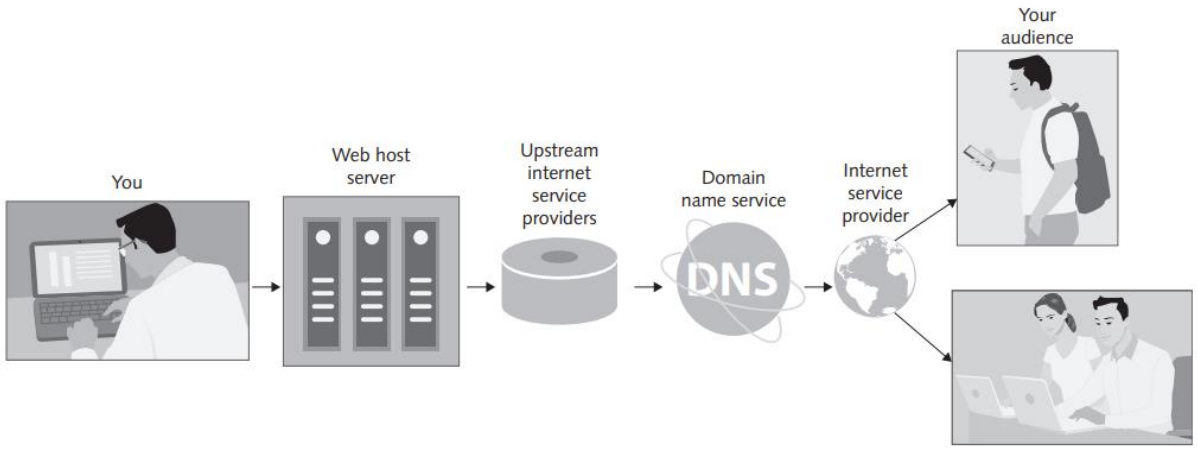
Internet software filters have also been developed to run on mobile devices such as Android, iPhone, and Microsoft smartphones, Television, Computers.

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, so users need not update their software. Such ISP, prevents access to known websites that address such topics as bomb making, gambling, hacking, hate, illegal drugs, pornography, profanity, public chat satanic activities, and suicide.

**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 (see Figure below) 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.



China has the largest online population in the world, with over 721 million Internet users. However, Internet censorship in China is perhaps the most rigorous in the world. The Chinese government blocks access to websites that discuss any of a long list of topics that are considered objectionable—including the Buddhist leader the Dalai Lama, anything to do with the government crackdown on the 1989 Tiananmen Square protests, and the banned spiritual movement Falun Gong. Chinese websites also employ censors who monitor and delete objectionable content. It is also said that the government even hires workers to post comments favorable to the government.

Brazilian government demands have closed more Google Gmail accounts and more blog sites than in any other country. In Brazil, filing a lawsuit to demand that Internet content be taken down is relatively easy and inexpensive. The ability of litigants to challenge content and demand that anonymous sources be revealed stifles Brazilian journalists and Internet bloggers.

In Cuba, only a few people can afford Internet access; Although Cuba has said it plans to double access in the next five years, the government continues to engage in censorship activities by frequently filtering and intermittently blocking websites that are critical of the state.

Reporters without Borders (RWB), an international nonprofit, nongovernmental organization with headquarters in Paris, promotes and defends freedom of information and freedom of the press around the world. Each year, RWB prepares an "Enemies of the Internet" list, which includes countries the group has determined have the highest levels of Internet censorship and surveillance. The United States and the United Kingdom were added to the 2014 edition of this list after information leaked by Edward Snowden revealed a high degree of government surveillance in both countries.

**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.

**Anonymity on the Internet**

Anonymous expression is the expression of opinions by people who do not reveal their identity. The freedom to express an opinion without fear of reprisal is an important right of a democratic society. Anonymity is even more important in countries that don't allow free speech. However, in the wrong hands, anonymous communication can be used as a tool to commit illegal or unethical activities.

Anonymous political expression played an important role in the early formation of the United States. Before and during the American Revolution, patriots who dissented against British rule often used anonymous pamphlets and leaflets to express their opinions. England had a variety of laws designed to restrict anonymous political commentary, and people found guilty of breaking these laws were subject to harsh punishment—from whippings to hangings. A famous case in 1735 involved a printer named John Zenger, who was prosecuted for seditious libel because he wouldn't reveal the names of anonymous authors whose writings he published. The authors were critical of the governor of New York. The British were outraged when the jurors refused to convict Zenger, in what is considered a defining moment in the history of freedom of the press in the United States.

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

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

Another landmark anonymity case involved a sailor threatened with discharge from the U.S. Navy because of information obtained from AOL. In 1998, following a tip, a Navy investigator asked AOL to identify the sailor, who used a pseudonym to post information in an online personal profile that suggested he might be gay. Thus, he could be discharged under the military's "don't ask, don't tell" policy, which was in effect at the time. AOL admitted that its representative violated company policy by providing the information.

A federal judge ruled that the Navy had overstepped its authority in investigating the sailor's sexual orientation and had also violated the Electronic Communications Privacy Act, which limits how government agencies can seek information from email or other online data. The sailor received undisclosed monetary damages from AOL and, in a separate agreement, was allowed to retire from the Navy with full pension and benefits.

**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.

In 2015, an American dentist shot and killed a lion named Cecil in Zimbabwe in a way that likely broke the law. Cecil was quite popular with visitors to the national park where he lived, and people around the world were upset by the news. Shortly after the dentist's identity was released, he became a victim of doxing. The URL for his practice's website and his work address and phone number were posted online and shared repeatedly across a variety of social networks. The dentist had his life threatened online, faced protesters outside his office, and had his vacation home in Florida vandalized.

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.

When an email is sent, the email software (for example, Outlook) automatically inserts information called a header on each packet of the message that identifies where the email originated from and who sent it. In addition, IP addresses are attached to the email and captured as the message transfers through various routers and relay servers. Internet users who want to remain anonymous can send email to an anonymous remailer service, which uses a computer program to strip the originating header and/or IP number from the message. It then forwards the message to its intended recipient—an individual, a chat room, or a newsgroup—with either no IP address or a fake one, ensuring that the header information cannot be used to identify the author. Some remailers route messages through multiple remailers to provide a virtually untraceable level of anonymity. Anonymous remailers do not keep any list of users and corresponding anonymizing labels used for them; thus, a remailer can ensure its users that no internal information has been left behind that can later be used to break identity confidentiality. Even if law-enforcement agencies serve a court order to release information, there is nothing to turn over.

The use of a remailer keeps communications anonymous; what is communicated, and whether it is ethical or legal, is up to the sender. The use of remailers by people committing unethical or even illegal acts in some states or countries has spurred controversy. Remailers are frequently used to send pornography, to illegally post copyrighted material to Usenet newsgroups, and to send unsolicited advertising to broad audiences (spamming). An organization's IT department can set up a firewall to prohibit employees from accessing remailers or to send a warning message each time an employee communicates with a remailer.

As part of an antiterrorist operation in late 2014, police in Spain raided 14 houses and social centers. Seven people arrested that day were held in a Madrid prison on suspicion of terrorism. The judge in the case cited three reasons for jailing the seven people—possession of certain books, including Against Democracy (a book that challenges the belief that the version of democracy practiced today is good and moral), the production of publications and forms of communication, and their use on an anonymous remailer to send emails. Many privacy experts believe that citing the use of secure email as a potential indicator of involvement in terrorist activities is an exceedingly dangerous precedent. As one blogger commented and many observers agree "Security is not a crime."

**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 applicant can request court permission to issue orders to command a person to appear under penalty. If the court grants permission, the applicant can serve orders 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 option is possible only when hate speech turns into clear threats and fear against specific citizens. Persistent or malicious harassment aimed at a specific person is hate speech, which can be prosecuted under the law, but general, broad statements expressing hatred of an ethnic, racial, or religious group cannot. A threatening private message sent over the Internet to a person, a public message displayed on a website describing intent to commit acts of hate-motivated violence against specific individuals, and libel directed at a particular person are all actions that can be prosecuted.

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

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

Because such prohibitions are included in the service contracts between ISPs and social networking sites and their subscribers and members—and do not involve the federal government—they do not violate anyone's First Amendment rights. Of course, people who lose an ISP or social networking account for violating the provider's regulations may resume their hate speech by simply opening a new account, either under a different name or with some other, more permissive site or ISP.

Gerardo Ortiz is an American regional Mexican singer-songwriter and record producer whose "Fuiste Mía" music video depicts him tossing his girlfriend into the trunk of his car and setting the car on fire after catching her with another man. The video was removed from YouTube following an online petition with over 6,000 signatures demanding the video be taken down for promoting and inciting violence against women. Ortiz defended the video as pure fiction where no one was actually harmed and compared it to content seen in movies and TV shows, but personally made the decision to have the video taken down at least temporarily. The video raises questions of artistic liberty and freedom of speech.

Although they may implement a speech code, public schools and universities are legally considered agents of the government and therefore must follow the First Amendment's prohibition against speech restrictions based on content or viewpoint. Corporations, private schools, and private universities, on the other hand, are not part of state or federal government. As a result, they may prohibit students, instructors, and other employees from engaging in offensive speech using corporate-, school-, or university-owned computers, networks, or email services.

Most other countries do not provide constitutional protection for hate speech. For example, promoting Nazi ideology is a crime in Germany, and denying the occurrence of the Holocaust is illegal in many European countries. Authorities in Britain, Canada, Denmark, France, and Germany have charged people for crimes involving hate speech on the web.

A U.S. citizen who posts material on the web that is illegal in a foreign country can be prosecuted if the person subjects himself or herself to the jurisdiction of that country—for example, by visiting there. As long as the person remains in the United States, that person is safe from prosecution because U.S. laws do not allow a person to be extradited for engaging in an activity protected by the U.S. Constitution, even if the activity violates the criminal laws of another country.

**Pornography on the Internet**

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

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

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

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

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

## 3.5 Social Networking Ethical Issues

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

Common features of social media are user accounts, profile pages (for individuals, groups, and businesses), friends or followers, event pages, news feeds, media-sharing features, like buttons, comments sections, and reviews—among others.

Different types of social media are blogs (with comments sections), discussion forums, media-sharing networks, wikis, social bookmarking tools, social messaging apps, and social networking, news, and shopping platforms.

**Social Networking Platforms**

A **social networking platform** creates an online community of Internet users that enables members to break down barriers created by time, distance, and cultural differences. Social networking platforms allow

people to interact with others online by sharing opinions, insights, information, interests, and experiences.

Some platforms, such as LinkedIn, are more text focused. Others, such as Instagram, Snapchat, Tumblr, and YouTube, are primarily focused on audio and visual content.

Members of an online social network may use the platform to interact with friends, family members, and colleagues—people they already know—but they may also make use of the platform to develop new personal and professional relationships. With the number of Internet users worldwide approaching 4 billion (just under 50 percent of the world population), there is an endless range of interests represented online, and a correspondingly wide range of social networking platforms catering to those interests.

**Business applications of social media**

Although many social networking platforms were originally targeted at nonbusiness users, many organizations now use social media tools to advertise, assess job candidates, and sell products and services.

An increasing number of business-oriented social networking platforms including Facebook, LinkedIn, Instagram, Twitter, Google/YouTube can be used to encourage and support relationships with consumers, clients, potential employees, suppliers, and business partners around the world.

With over 1.1 billion unique visitors each month, Facebook includes the largest blend of demographics of all the social networks. It is a massive social media platform that provides online marketing tools that make it easier for organizations to develop marketing campaigns and reach their target audience. Organizations can use Facebook as a platform to promote and inform customers about their latest initiatives and promotions.

Companies can use LinkedIn, the world's largest professional network, to develop contacts with clients, promote themselves, and connect with individuals and organizations within their industry. It can also be used to find highly skilled employees and contractors. LinkedIn Groups enables organizations to create groups to target a particular industry position, and then invite LinkedIn members in the target group to join.

Twitter enables an organization to share short text updates, images, links, polls, and videos. Hashtags, which can be used to quickly spread a company's message, allow a company's tweets to be seen not only by its followers but also by those who are interested in the topic being tweeted about. For instance, a hashtag with a product name allows anyone interested in the product to see the tweet regardless of whether they are following the company.

**Social Media Marketing**

Social media marketing involves the use of social networks to communicate and promote the benefits of products and services. According to Nielsen, about 37 percent of all consumers say they use social media to find out about products and services, while about 32 percent use social media to receive exclusive offers, coupons, or other discounts from brands. The two primary objectives of social media marketers are raising brand awareness and driving traffic to a website to increase product sales. Other important benefits of social media marketing are developing loyal fans, providing market insight, and generating leads. Two significant advantages of social networking marketing over more traditional media—such as radio, TV, and newspapers—are that marketers can create an opportunity to generate a conversation with viewers of the message, and those messages can be targeted to reach people with the desired

demographic characteristics. The overwhelming majority of social media marketers use Facebook ads (87%), Google ads (39%), Twitter ads (19%), and LinkedIn ads (17%) are the next most popular.

**Paid media marketing** involves paying a third party to broadcast an organization's display ads or sponsored messages to social media users. An organization can acquire paid social media traffic through social media ads on Facebook, LinkedIn, Twitter, YouTube, and many other social media marketing channels. Paid media marketing enables an organization to target a specific audience—based on demographics and other factors—to increase the percentage of their target audience that is exposed to its content.

**Earned media** refers to the media exposure an organization gets through press and social media mentions, positive online ratings, and reviews, tweets and retweets, reposts (or "shares"), recommendations, and so on. Earned social media traffic enables an organization to reach more people without any additional cost. The volume of earned media is also a factor in determining how high an organization ranks in Google's search engine.

**Viral marketing** is an approach to social media marketing that encourages individuals to pass along a marketing message to others, thus creating the potential for exponential growth in the message's exposure and influence as one person tells two people, each of those two people tell two or three more people, and so on. The goal of a viral marketing campaign is to create a buzz about a product or idea that spreads wide and fast.

**Social Media in the Hiring Process**

According to CareerBuilder, 60 percent of employers used social media to research job candidates in 2016. Nearly half of those companies found information on social media that gave a negative impression of the candidate. The offending content included inappropriate photographs and videos, information about the candidate drinking or using drugs, and discriminatory comments related to gender, race, and religion. Social media users frequently provide sex, age, marital status, sexual orientation, religion, and political affiliation data in their profiles. Users who upload personal photos may reveal a disability or their race or ethnicity; therefore, without even thinking about it, an individual may have revealed data about personal characteristics that are protected by civil rights legislation. Employers can legally reject a job applicant based on the individual's social media activity only if the company is not violating federal or state discrimination laws.

For example, an employer cannot legally screen applicants based on race or ethnicity. Or suppose that by checking a social networking site, a hiring manager finds out that a job candidate is pregnant and makes a decision not to hire that person based on that information. That employer would be at risk of a job employment discrimination lawsuit because refusing to hire on the basis of pregnancy is prohibited.

Job seeking candidates should review their presence on social media and remove photos and postings that portray them in a potentially negative light. Many jobseekers delete their social media accounts altogether because they know employers check such sites. Jobseekers must realize that pictures and words posted online, once intended for friends only, can reach a much larger audience and can have an impact on their job search.

**Improving Customer Service Using Social Media**

In the past, companies relied heavily on their market research and customer service organizations to provide them with insights into what customers think about their products and services. For example,

many consumer goods companies put toll-free numbers on their products so that consumers could call in and speak with trained customer service representatives to share their comments and complaints.

Increasingly, however, consumers are using social networks to share their experiences, both good and bad, with others. And the old saying “A happy customer tells a few people, an unhappy customer tells everyone” has never been more true. Customers also use social media to seek advice on how to use products more effectively and how to deal with special situations encountered when using a product.

Global market research company J.D. Power claims that two-thirds of consumers have used a company’s social media channel for customer service. Many of these consumers have very high expectations: larger percent feel they should receive a response with an hour. Unless organizations actively monitor and engage with customers on social media, their customers may be left to resolve their issues and questions on their own, often in ways that are not ideal. The end result can be dissatisfaction with the product and loss of customers and future sales. Thus, progressive companies are focusing more resources on monitoring issues and assisting customers via social media.

**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. Nearly three-quarters (72 percent) of U.S. Internet users have witnessed online harassment or abuse, and almost half (47 percent) have personally experienced cyberabuse.

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. Overall, 8 percent of U.S. Internet users say they have experienced cyberstalking to the point of feeling unsafe or afraid. Young people, especially women under 30, are more likely to be targets of cyberstalking. It is estimated that 14 percent of Internet users under 30 year of age have been cyberstalked, including 20 percent of women under 30.

The cyberharassment differs from cyberstalking in that it is aimed at disturbing an individual but does not involve a credible threat of physical harm.

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

**Encounters with Sexual Predators**

Some social networking platforms, law enforcement, and the courts have been criticized for not doing enough to protect minors from encounters with sexual predators. Most law enforcement officers understand that dangers exist in not mandating Internet restrictions for repeat sex offenders but also realize that creating a national policy would be difficult because even convicted felons have first amendment rights. A federal court ruled in early 2013 that an Indiana state law that prohibited use of social networks by registered sex offenders violated the First Amendment rights of the sex offenders and was unconstitutional. Similar laws in Nebraska and Louisiana have also been ruled unconstitutional. Eight other states have enacted laws that in some way restrict the use of the Internet by sex offenders. 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.

**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.

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

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

**Miscellaneous Social Media Issues**

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

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

Social media platforms also enable a degree of self-image manipulation. For example, Snapchat provides filters that alter the user's face by smoothing and whitening skin, changing eye shape, nose size, and jaw profile. Some users favor the filters because they enable users to feel more confident posting their photo while others feel that the filters promote an unrealistic and Westernized standard of beauty.

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

- Social media are web-based communication channels and tools that enable people to interact with each other by creating online communities where they can share information, ideas, messages, and other content, including images, audio, and video.
- A social networking platform creates an online community of Internet users that enables members to break down barriers created by time, distance, and cultural differences; such a site allows people to interact with others online by sharing opinions, insights, information, interests, and experiences.
- The number of Internet users worldwide is approaching 4 billion or roughly half the population.
- Many organizations employ social networking platforms to advertise, identify and access job candidates, improve customer service, and sell products and services.
- An increasing number of business-oriented social networking platforms are designed to encourage and support relationships with consumers, clients, potential employees, suppliers, and business partners around the world.

- Social media marketing involves the use of social networks to communicate and promote the benefits of products and services.
- Two significant advantages of social media marketing over traditional marketing are that marketers can create a conversation with viewers of their ads and that ads can be targeted to reach people with the desired demographic characteristics.
- Social media marketing involves the use of social networks to communicate and promote the benefits of products and services. The two primary objectives of social media marketers are raising brand awareness and driving traffic to a website to increase product sales.
- Organic media marketing employs tools provided by or tailored for a particular social media platform to build a social community and interact with it by sharing posts and responding to customer comments on the organization's blog and social media accounts.
- Paid media marketing involves paying a third party to broadcast an organization's display ads or sponsored messages to social network users. Two common methods of charging for paid media are cost per thousand impressions and cost per click.
- Earned media refers to media exposure an organization gets through press and social media mentions, positive online ratings and reviews, tweets and retweets, reposts (or "shares"), recommendations, and so on. Earned social media traffic enables an organization to reach more people without any additional cost.
- Viral marketing is an approach to social media marketing that encourages individuals to pass along a marketing message to others, thus creating the potential for exponential growth in the message's exposure and influence.
- Some 60 percent of employers used social media to research job candidates with half of those finding information that gave a negative impression of the candidate.
- Employers can legally reject a job applicant based on the contents of the individual's social networking profile as long as the company is not violating federal or state discrimination laws.
- Job seeking candidates should review their presence on social media and remove photos and postings that portray them in a potentially negative light. Many jobseekers delete their social media accounts altogether.
- Increasingly, consumers are using social networks to share their experiences, both good and bad, with others. Because of this, many organizations actively monitor social media networks as a means of improving customer service, retaining customers, and increasing sales.
- A social shopping platform brings shoppers and sellers together in a social networking environment in which members share information and make recommendations while shopping online.

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

- Cyberabuse is any form of mistreatment or lack of care, both physical and mental, based on the use of an electronic communications device that causes harm and distress to others.
- Nearly three-quarters of U.S. Internet users have witnessed online harassment or abuse and almost half have personally experienced it.
- Cyberharassment is a form of cyberabuse in which the abusive behavior, which involves the use of an electronic communications device, is degrading, humiliating, hurtful, insulting, intimidating, malicious, or otherwise offensive to an individual or group of individuals causing substantial emotional distress.

- Cyberstalking is also a form of cyberabuse that consists of a long-term pattern of unwanted persistent pursuit and intrusive behavior (involving the use of an electronic communications device) that is directed by one person against another that causes fear and distress in the victim.
- The National Center for Victims of Crime offers tips on how to combat cyberstalking.
- The 1994 Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act set requirements for sex offender registration and notification in the United States. It also that states create websites that provide information on sex offenders within the state.
- The Sex Offender Registration and Notification Provisions (SORNA) of the Adam Walsh Child Protection and Safety Act of 2006 set national standards that govern which sex offenders must register and what data must be captured.
- Most social networking platforms have terms of use agreements, a privacy policy, or a content code of conduct that summarizes key legal aspects regarding use of the platform. Typically, the terms state that the platform has the right to delete material and terminate user accounts that violate its policies. These policies can be difficult to enforce.
- Inappropriate material posted online includes nonconsensual posts that include intimate photos or videos of people without their permission; such posts are often referred to as “revenge porn.” This type of content is often uploaded by ex-partners with an intention to shame, embarrass, and/or harass their former partner.
- The First Amendment of the U.S. Constitution protects the right of freedom of expression from government interference, however, it does not prohibit free speech interference by private employers.
- Organizations should put in place a social media policy to avoid legal issues and set clear guidelines and expectations for employees.
- The increased risk of accidents associated with social media interaction while driving, the tendency of many social media users to become narcissist in their postings, and the ability to perform self-image manipulation are additional social media issues.