CHAPTER 5

FREEDOM OF EXPRESSION

QUOTE

If we don't believe in freedom of expression for people we despise, we don't believe in it at all.

—Noam Chomsky, American linguist, philosopher, cognitive scientist, historian, social critic, and political activist

Marcos Mesa Sam Wordley/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

Around the world, Internet censorship and surveillance is on the rise, fueling concerns regarding issues such as freedom of expression, privacy rights, free and fair elections, and corruption. For instance, political and human rights activists in Brazil, China, Ethiopia, Greece, India, Indonesia, Iran, Russia, Saudi Arabia, Turkey, Uganda, and Zimbabwe all are subject to particularly strong censorship and suppression. And in many countries, journalists, as well as their sources, are the targets of

censorship and surveillance activities by those working on behalf of politicians, government entities, and criminals.

Faced with the reality of online censorship and surveillance, many activists, journalists, and whistle-blowers—among others—feel an increased need to keep their Internet activities concealed from the government, Internet service providers, and website operators. Those concerns were only heightened following the release of information regarding the U.S. government's surveillance activities that came to light with Edward Snowden's leak of National Security Agency documents in 2013.

One tool available for those looking for more online privacy and protection is Tor, which is marketed as a free software and an open network that can safeguard users from network surveillance that threatens their "personal freedom and privacy, confidential business activities and relationships, and state security." Tor works by bouncing Internet communications around a network of servers distributed around the world, thus thwarting anyone who is trying to monitor the user's Internet connection to learn what sites he or she is visiting while also preventing the sites being visited from establishing the user's physical location. Tor also allows website operators to publish websites without revealing their location.[1]

With features that enable users to access information, communicate freely, and form and discover communities of support in potentially dangerous environments, Tor is one example of how technology can be employed to serve the causes of freedom, safety, liberty, and human rights for people around the world. However, a recent study found that 57 percent of the sites designed for Tor are used by people engaged in criminal activity, including drugs, illicit finance, and extreme pornography.[2] What measures are available to defeat Internet censorship and surveillance so that Internet users can truly enjoy freedom of expression? Can technology be used to support the actions of "good actors" without aiding "bad actors" as well?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What is the basis for the protection of freedom of expression in the United States, and what types of expressions are not protected under the law?
2. What are some key federal laws that affect online freedom of expression, and how do they impact organizations?
3. What important freedom of expression issues relate to the use of information technology?

FIRST AMENDMENT RIGHTS

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

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

The right to freedom of expression is one of the most important rights for free people everywhere. The **First Amendment** to the U.S. Constitution (shown in Figure 5-1) was

Kasia/Shutterstock.com

FIGURE 5-1 The U.S. Constitution

adopted to guarantee this right and others. Over the years, a number of federal, state, and local laws have been found unconstitutional because they violated one of the tenets of this amendment.

The First Amendment reads as follows:

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

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

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

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

Obscene Speech

Miller v. California is the 1973 Supreme Court case that established a test to determine if material is obscene and therefore not protected by the First Amendment. After conducting a mass mailing campaign to advertise the sale of adult material, Marvin Miller was convicted of violating a California statute prohibiting the distribution of obscene material. Some unwilling recipients of Miller's brochures complained to the police, initiating the legal proceedings. Although the brochures contained some descriptive printed material, they primarily consisted of pictures and drawings explicitly depicting men and women engaged in sexual activity. In ruling against Miller, the Supreme Court determined that speech can be considered obscene and not protected under the First Amendment based on the following three questions:

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

These three tests have become the U.S. standard for determining whether something is obscene. The requirement that a work be assessed by its impact on an average adult in a community has raised many questions:

- Who is an average adult?
- What are contemporary community standards?
- What is a community? (This question is particularly relevant in cases in which potentially obscene material is displayed worldwide via the Internet.)

Defamation

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

A woman sued Gawker Media (a controversial, now-defunct, website that trafficked in news, gossip, and opinion) and its founder for defamation and invasion of privacy. She claimed that a Gawker's blog post speculating that she was dating her boss at tech company Yahoo damaged her reputation and caused her to suffer personally and professionally by stating that she did not conduct herself professionally and ethically and exercised poor judgment in her senior position in the firm's human resources organization.[3]

CRITICAL THINKING EXERCISE: POSTING A NEGATIVE REVIEW ON YELP

Your friend recently had an unpleasant experience at a local eatery where the service was poor and the food overpriced. In addition, she became ill with severe stomach cramps within hours of eating at the restaurant. She has drafted a scathing review and plans to post it on Yelp, accusing the restaurant of giving her food poisoning. She has asked you to look over her review before posting it. What would you say?

FREEDOM OF EXPRESSION: KEY ISSUES

Information technology has provided amazing new ways for people to communicate with others around the world, but with these new methods come new responsibilities and new ethical dilemmas. This section discusses a number of key issues related to the freedom of expression, including controlling access to information on the Internet, Internet censorship, SLAPP lawsuits, anonymity on the Internet, John Doe lawsuits, hate speech, pornography on the Internet, and fake news reporting.

Controlling Access to Information on the Internet

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

Communications Decency Act

The Telecommunications Act (Public Law 104-104) became law in 1996. Its primary purpose was to allow free competition among phone, cable, and TV companies. The act was broken into seven major sections or titles. Title V of the Telecommunications Act was the **Communications Decency Act (CDA)**, aimed at protecting children from pornography. The CDA imposed $250,000 fines and prison terms of up to two years for the transmission of "indecent" material over the Internet.

In February 1996, the American Civil Liberties Union (ACLU) and 18 other organizations filed a lawsuit challenging the criminalization of so-called indecency on the web under the CDA. The problem with the CDA was its broad language and vague definition of *indecency*, a standard that was left to individual communities to determine. In June 1997, the Supreme Court ruled the law unconstitutional and declared that the Internet must be afforded the highest protection available under the First Amendment.[4] 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."[5] 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" (47 U.S.C. § 230). This provides immunity to an Internet service provider (ISP) that publishes user-generated content, as long as its actions do not rise to the level of a content provider. In general, the closer an ISP is to a pure service provider than to a content provider, the more likely that the Section 230 immunity will apply.[6] This portion of the CDA protects social networking companies such as Facebook and Twitter from defamation suits in connection with user postings that appear on their sites.

Facebook presents a constantly updated list of stories, called the News Feed, in the middle of each Facebook user's home page. Using an algorithm based on each user's Facebook activity and connections, the social networking site attempts to choose the "best" content out of several thousand potential stories, placing those near the top of the News

Feed. The number of comments and likes a post receives, as well as what type of story it is (e.g., photo, video, news article, or status update), influences whether and how prominently a story will appear in a user's News Feed. Facebook also conducts surveys and focus groups to get input on what stories people think should appear. The more engaging the content, the more time users will spend on Facebook and the more often they will likely return to the site. This enables Facebook to earn more revenue from ads shown in News Feed content.[7]

Because one of the traditional roles of a publisher is to select which stories to show its readers, Facebook's efforts to shape the news that its users see could result in it being viewed as an information content provider by the courts, resulting in a loss of protection under Section 230 of the CDA. If that were to happen, Facebook could become liable for defamation based on the postings of its subscribers.

Child Online Protection Act

In October 1998, the **Child Online Protection Act (COPA)** was signed into law. This act is not to be confused with the Children's Online Privacy Protection Act (COPPA) that is directed at websites that want to gather personal information from children under the age of 13. COPA states that "whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both."[8]

After its passage, COPA became a rallying point for proponents 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.[9] 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.

According to TopTenREVIEWS, the top rated Internet filters for home users for 2016 include Net Nanny, SpyAgent, and Qustodio.[10] Safe Eyes from InternetSafety.com is an Internet-filtering software that filters videos on YouTube, manages the viewing of online TV using age-appropriate ratings (e.g., TV-G and TV-PG), and blocks the use of media-sharing applications used to download pirated music and videos (see Figure 5-2). Internet software filters have also been developed to run on mobile devices such as Android, iPhone, and Microsoft smartphones.

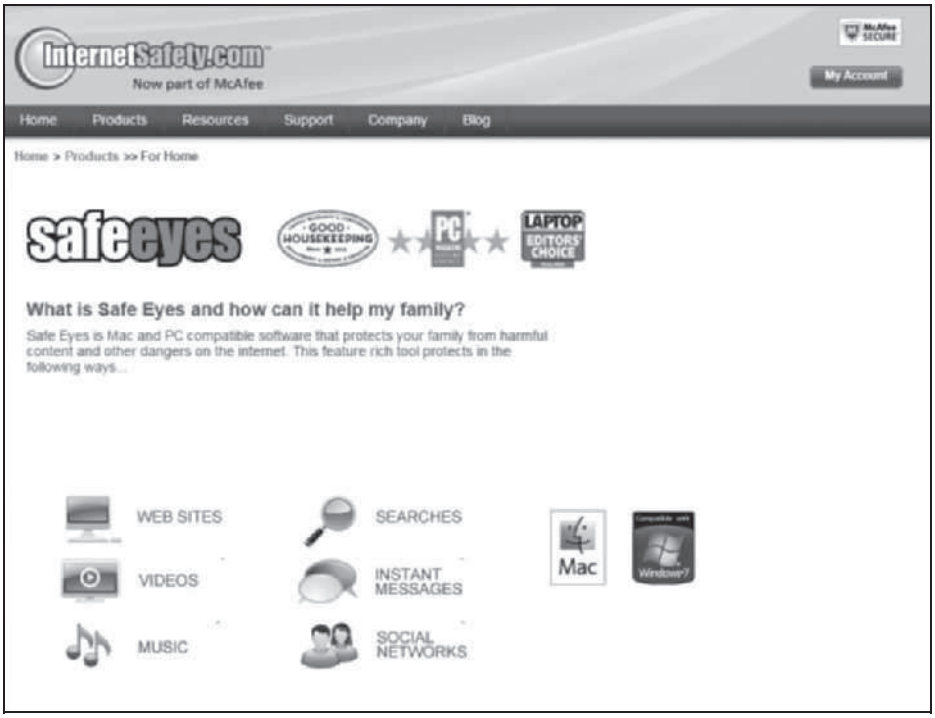

FIGURE 5-2 Screenshot of Safe Eyes from Internet Safety

Source: InternetSafety.com, part of McAfee Inc.

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. One such ISP, ClearSail/Family.NET, 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. ClearSail employees search the web daily to uncover new sites to add to ClearSail's block list. The ISP blocks specific URLs and known pornographic-hosting services, as well as other sites based on certain keywords. ClearSail's filtering blocks millions of web pages. Newsgroups are also blocked because of the potential for pornography within them.[11]

Children's Internet Protection Act

In another attempt to protect children from accessing pornography and other explicit material online, Congress passed the **Children's Internet Protection Act (CIPA)** in 2000. The act required federally financed schools and libraries to use some form of technological protection (such as an Internet filter) to block computer access to obscene material, pornography, and anything else considered harmful to minors. Congress did not specifically define what content or websites should be forbidden or what measures should be used—these decisions were left to individual school districts and library systems. Any school or library that failed to comply with the law would no longer be eligible to receive federal money through the E-Rate program, which provides funding to help pay for the cost of Internet connections. The following points summarize CIPA:

- Under CIPA, schools and libraries subject to CIPA will not receive the discounts offered by the E-Rate program unless they certify that they have certain Internet safety measures in place to block or filter pictures that are obscene, contain child pornography, or are harmful to minors (for computers used by minors).
- Schools subject to CIPA are required to adopt a policy to monitor the online activities of minors.
- Schools and libraries subject to CIPA are required to adopt a policy addressing access by minors to inappropriate matter online; the safety and security of minors when using email, chat rooms, and other forms of direct electronic communications; unauthorized access, including hacking and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal information regarding minors; and restricting minors' access to materials harmful to them. CIPA does not require the tracking of Internet use by minors or adults.[12]

Opponents of the law were concerned that it transferred power over education to private software companies who develop the Internet filters and define what sites to block. Furthermore, opponents felt that the motives of these companies were unclear—for example, some filtering companies track students' online activities and sell the data to market research firms. Opponents also pointed out that some versions of these filters were ineffective, blocking access to legitimate sites and allowing access to objectionable ones. Yet another objection was that penalties associated with the act could cause schools and libraries to lose federal funds from the E-Rate program, which is intended to help bridge the digital divide between rich and poor, urban and rural. Loss of federal funds would lead to a less capable version of the Internet for students at poorer schools, which have the fewest alternatives to federal aid.

CIPA's proponents contended that shielding children from drugs, hate speech, pornography, and other topics was a sufficient reason to justify filters. They argued that

Internet filters are highly flexible and customizable and that critics exaggerated the limitations. Proponents pointed out that schools and libraries could elect not to implement a children's Internet protection program; they just wouldn't receive federal money for Internet access.

Many school districts implemented programs consistent with CIPA. Acceptance of an Internet filtering system is more meaningful if the system and its rationale are first discussed with parents, students, teachers, and administrators. Then the program can be refined, taking into account everyone's feedback. An essential element of a successful program is to require that students, parents, and employees sign an agreement outlining the school district's acceptable-use policies for accessing the Internet. Controlling Internet access via a central district-wide network rather than having each school set up its own filtering system reduces administrative effort and ensures consistency. Procedures must be defined to block new objectionable sites as well as remove blocks from websites that should be accessible.

Implementing CIPA in libraries is much more difficult because a library's services are open to people of all ages, including adults who have First Amendment rights to access a broader range of online materials than are allowed under CIPA. In *United States, et al. v. American Library Association, Inc., et al.*, the American Library Association challenged CIPA. Ultimately in that case, the Supreme Court made it clear that the constitutionality of government-mandated filtering schemes depends on adult patrons' ability to request and receive unrestricted access to protected speech.[13] A possible compromise for public libraries with multiple computers would be to allow unrestricted Internet use for adults but to provide computers with only limited access for children.

Rather than deal with all the technical and legal complications, some librarians say they wish they could simply focus on training students and adults to use the Internet safely and wisely.

Digital Millennium Copyright Act

The **Digital Millennium Copyright Act (DMCA)**, which was signed into law in 1998, addresses a number of copyright-related issues. The DMCA is divided into five titles that will be discussed more fully in Chapter 6. Title II, the "Online Copyright Infringement Liability Limitation Act," provides limitations on the liability of an ISP for copyright infringement that can arise when an ISP subscriber posts copyrighted material such as audio tracks, videos, books, and news articles on the Internet. Its passage amended Title 17 of the U.S. Code (Copyright) by adding a new Section 512, which says that an ISP cannot be held liable for copyright infringement if, when notified by the copyright holder, it notifies the subscriber of the alleged infringement and executes a "takedown" by removing the offending content.[14] The fact that the content was created by you, or in the case of a photo or video the subject is you, can be sufficient enough to request a takedown.

A woman posted a 29-second video on YouTube of her baby dancing in the kitchen with Prince's "Let's Go Crazy" playing in the background. Universal Music Corporation sent YouTube a DMCA takedown notice claiming use of its song constituted copyright infringement. The video was initially removed from YouTube for a few weeks but was eventually reinstated. The case has been in the courts for over seven years and has raised the issue that copyright owners need to consider fair use before they issue a DMCA takedown notice. (Fair use is the copying of copyrighted material done for a limited and

"transformative" purpose, such as to comment upon, criticize, or parody a copyrighted work. Fair use can be done without permission from the copyright owner and is a defense against copyright infringement).[15]

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 5-3) with each intermediary vulnerable to some degree of pressure from those who want to silence the speaker. Web hosting services are often the recipients of defamation or copyright infringement claims by government authorities or copyright holders, demanding the immediate takedown of hosted material that is deemed inappropriate or illegal. Government entities may pressure "upstream" Internet service providers to limit access to certain websites, allow access to only some content or modified content at certain websites, reject the use of certain keywords in search engines, and track and monitor the Internet activities of individuals. Several countries have enacted the so-called three-strikes laws that require ISPs to terminate a user's Internet connection once that user has received a number of notifications of posting of content deemed inappropriate or illegal. Censorship efforts may also focus on Domain Name System (DNS) servers, which convert human-readable host and domain names into the machine-readable, numeric Internet Protocol (IP) addresses that are used to point computers and other devices toward the correct servers on the Internet. Where authorities have control over DNS servers, officials can "deregister" a domain that hosts content that is deemed inappropriate or illegal so that the website is effectively invisible to users seeking access to the site.

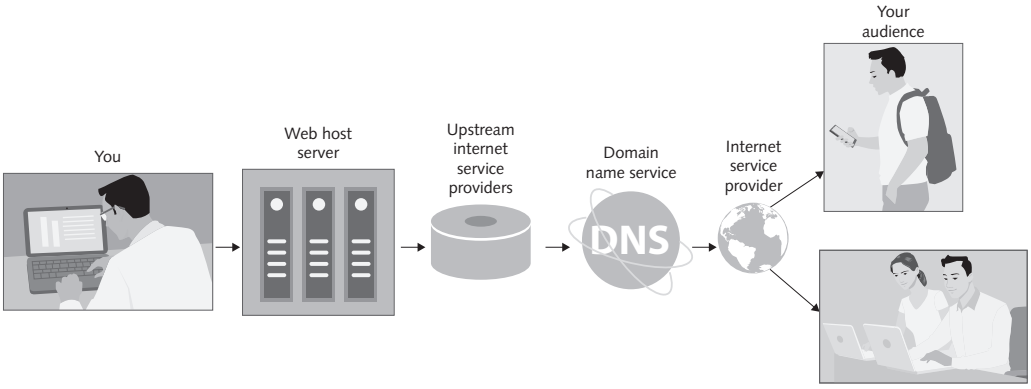

FIGURE 5-3 Internet Censorship

China has the largest online population in the world, with over 721 million Internet users (see Table 5-1, which depicts the top 10 countries in terms of number of 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. The government even hires workers to post comments favorable to the government.[16]

TABLE 5-1 The top 10 countries with the highest number of Internet users (2016)

Rank	Country	Internet users (millions)	Population (millions)	Penetration (% of population)
1	China	721	1,382	52
2	India	462	1,327	35
3	United States	287	324	89
4	Brazil	139	210	66
5	Japan	115	126	91
6	Russia	102	143	71
7	Nigeria	86	187	46
8	Germany	71	81	88
9	United Kingdom	60	65	93
10	Mexico	58	129	45

Source: Internet Users by Country (2016), *Internet Live Stats*, www.internetlivestats.com/internet-users-by-country.

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.[17]

In Cuba, only a few people can afford Internet access; currently, only 5 percent of homes are connected. 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.[18]

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.[19]

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.[20]

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.[21] 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.[22]

Anti-SLAPP laws are designed to reduce frivolous SLAPPs. As of 2015, 28 states and the District of Columbia had passed anti-SLAPP legislation to protect people who are the target of a SLAPP.[23] Typically, under such legislation, a person hit with what they deem to be a SLAPP can quickly file an anti-SLAPP motion, which puts a hold on the original lawsuit until the court determines whether the defendant was being targeted for exercising free-speech rights, petitioning the government, or speaking in a public forum on "an issue of public interest." In such cases, the SLAPP lawsuit is thrown out unless the plaintiff can show that the claims are legitimate and likely to succeed at trial. To guard against abusive anti-SLAPP motions, the side that loses such a case is required to pay the other side's legal fees.[24]

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.[25]

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.[26]

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."[27]

John Doe Lawsuits

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

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

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

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

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

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

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

The EFF represented two of the John Does whose identities were subpoenaed. EFF attorneys argued that the message board postings cited by PPLS revealed no company secrets but were merely disparaging the company and its treatment of sales associates. They argued further that requiring the John Does to reveal their identities would let the company punish them for speaking out and set a dangerous precedent that would discourage other Internet users from voicing criticism. Without proper safeguards on John Doe subpoenas, a company could use the courts to uncover its critics.

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

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

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

Hate Speech

In the United States, speech that is merely annoying, critical, demeaning, or offensive enjoys protection under the First Amendment. Legal recourse is possible only when hate speech turns into clear threats and intimidation against *specific* citizens. Persistent or malicious harassment aimed at a specific person is **hate speech**, which can be prosecuted under the law, but general, broad statements expressing hatred of an ethnic, racial, or religious group cannot. A threatening private message sent over the Internet to a person, a public message displayed on a website describing intent to commit acts of hate-motivated violence against specific individuals, and libel directed at a particular person are all actions that can be prosecuted.

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

To post videos on YouTube, you must first create a YouTube or a Google account (Google is the owner of YouTube) and agree to abide by the site's published guidelines.[30] The YouTube guidelines prohibit the posting of videos showing such things as pornography, animal abuse, graphic violence, predatory behavior, and drug use. The guidelines also prohibit the posting of copyrighted material—such as music, television programs, or movies—that is owned by a third party. YouTube staff members review user-posted videos on a regular basis to find any that violate the site's community guidelines. Those that violate the guidelines are removed. Certain other videos are age-restricted because of their content. Users are penalized for serious or repeated violations of the guidelines and can have their account terminated.[31]

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.[32] The video raises questions of artistic liberty and freedom of speech.[33]

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.[34] Access via the Internet enables pornography consumers to avoid offending others or being embarrassed by others observing their purchases. There is no question that online adult pornography is big business (revenue estimates vary widely between $1 billion and $97 billion) and generates a lot of traffic; it is estimated that there are over 72 million visitors to pornographic websites monthly.[35,36]

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

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

U.S. organizations must be very careful when dealing with issues relating to pornography in the workplace. By providing computers, Internet access, and training in how to use those computers and the Internet, companies could be seen by the law as purveyors of pornography because they have enabled employees to store pornographic material and retrieve it on demand. Nielsen has found that 25 percent of working adults admit to looking at pornography on a computer at work.[39] In addition, if an employee sees a coworker viewing porn on a workplace computer, that employee may be able to claim that the company has created a hostile work environment. Such a claim opens the organization to a sexual harassment lawsuit that can cost hundreds of thousands of dollars and tie up managers and executives in endless depositions and court appearances.

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

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

Numerous federal laws address issues related to child pornography—including laws concerning the possession, production, distribution, or sale of pornographic images or

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

Sexting—sending sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone—is a fast-growing trend among teens and young adults. A Drexel University survey of college students revealed that 54 percent had sent or received "sexually explicit text messages or images" when they were under age 18. Previous studies had pegged the number much lower—around 20 percent. Students in this study may have been more honest because they were allowed to remain anonymous and were reporting on past behavior.[40]

Increasingly, people who take part in sexting are suffering the consequences of this fad. Once an image or video is sent, there is no taking it back and no telling to whom it might be forwarded. And it is not just teenagers who participate in sexting. Consider quarterback Bret Favre and U.S. representative Anthony Weiner who were both parties to embarrassing sexting episodes. Sexters can also face prosecution for child pornography, leading to possible years in jail and decades of registration as a sex offender. Some states have adopted laws that prescribe penalties aimed specifically at teenagers engaged in sexting. These laws make the penalties for teen sexting less severe than if an adult would send similar photos to an under-age person.

Controlling the Assault of Non-Solicited Pornography and Marketing Act

The **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** (15 U.S.C. § 7704) specifies requirements that commercial emailers must follow when sending messages that have a primary purpose to advertise or promote a commercial product or service. The key requirements of the law include:

- The *From* and *To* fields in the email, as well as the originating domain name and email address, must be accurate and identify the person who initiated the email.
- The subject line of the email cannot mislead the recipient as to the contents or subject matter of the message. In addition, if the message contains sexually oriented material, the phrase "SEXUALLY EXPLICIT" must appear in capital letters as the first characters in the subject line.
- The email must be identified as an advertisement and include a valid physical postal address for the sender.
- The emailer must provide a return email address or some other Internet-based response procedure to enable the recipient to request no future emails, and the emailer must honor such requests to opt out.
- The emailer has 10 days to honor the opt-out request.

- Additional rules prohibit the harvesting of email addresses from websites, using automated methods to register for multiple email accounts, or relaying email through another computer without the owner's permission.

Messages whose primary purpose is to communicate information about a specific transaction or relationship between the sender and recipient are not subject to the CAN-SPAM Act. Thus, a message regarding an attempt to deliver a legitimately placed online order or information about a product recall would be exempt.

Each violation of the provisions of the CAN-SPAM Act can result in a fine of up to $250 for each unsolicited email, and fines can be tripled in certain cases. A Canadian spammer was ordered to pay $873 million in fines for allegedly spamming Facebook accounts with over four million posts. Of course, the spammer could not pay the fine and instead declared bankruptcy.[41]

The Federal Trade Commission (FTC) is charged with enforcing the CAN-SPAM Act, and the agency maintains a consumer complaint database relating to the law. Consumers can submit complaints online at *www.ftc.gov* or forward email to the FTC at *spam@use.gov*. Other countries have their own version of the CAN-SPAM Act.

The CAN-SPAM Act can also be used in the fight against the dissemination of pornography. For example, two men were indicted by an Arizona grand jury for violating the CAN-SPAM Act by sending massive amounts of unsolicited email advertising pornographic websites. They had amassed an email database of 43 million people and used it to send emails containing pornographic images. AOL stated it received over 660,000 complaints from people who received spam from the two, whose operation was highly profitable—enabling the two men to earn over $1.4 million in 2003. The defendants ran afoul of the CAN-SPAM Act by sending messages with false return addresses and for using domain names registered using false information. They were convicted of multiple counts of spamming and criminal conspiracy, which carry a maximum sentence of five years each plus a fine of $500,000 and up to 20 years for money laundering. This is believed to be the first conviction involving CAN-SPAM Act violations.[42] A man nicknamed the Spam King was sentenced to 2½ years in prison and fined $310,000 for sending some 27 million spam emails to Facebook users. He was not prosecuted under the CAN-SPAM Act but instead was found guilty of federal charges including fraud and criminal contempt in connection with using electronic mail.[43]

There is considerable debate over whether the CAN-SPAM Act has helped control the growth of spam. After all, the act clearly defines the conditions under which the sending of spam is legal, and as long as mass emailers meet these requirements, they cannot be prosecuted. Some suggest that the act could be improved by penalizing the companies that use spam to advertise, as well as ISPs who support the spammers.

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).[44] 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.

Table 5-2 provides a manager's checklist for dealing with issues of freedom of expression in the workplace. In each case, the preferred answer is *yes*.

TABLE 5-2 Manager's checklist for handling freedom of expression issues in the workplace

Question	Yes	No
Do you have a written data privacy policy that is followed?		
Does your corporate IT usage policy discuss the need to conserve corporate network capacity, avoid legal liability, and improve worker productivity by limiting the nonbusiness use of information resources?		
Did the developers of your policy consider the need to limit employee access to nonbusiness-related websites (e.g., Internet filters, firewall configurations, or the use of an ISP that blocks access to such sites)?		
Does your corporate IT usage policy discuss the inappropriate use of anonymous remailers?		
Has your corporate firewall been set to detect the use of anonymous remailers?		
Has your company (in cooperation with legal counsel) formed a policy on the use of John Doe lawsuits to identify the authors of libelous, anonymous email?		
Does your corporate IT usage policy make it clear that defamation and hate speech have no place in the business setting?		
Does your corporate IT usage policy prohibit the viewing and sending of pornography?		
Does your corporate acceptable use policy communicate that employee email is regularly monitored for defamatory, hateful, and pornographic material?		
Does your corporate IT usage policy tell employees what to do if they receive hate mail or pornography?		

CRITICAL THINKING EXERCISE: FILING A JOHN DOE LAWSUIT

You are a young, recently graduated attorney working part-time as part of the re-election campaign team for your midsized city's mayor. Several citizens have taken to writing strongly worded anonymous letters to the local newspaper voicing their disagreement over your candidate's actions in her initial term as mayor. The campaign manager has suggested that you file John Doe lawsuits against the most vocal complainers as a warning to others of what they can expect if they are too vocal in their disagreement with the mayor. The goal is to intimidate others who might be inclined to write negative letters to the newspaper. Do you think this tactic will be successful? Why or why not?

Summary

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

- The First Amendment protects Americans' rights to freedom of religion, freedom of expression, and freedom to assemble peaceably. The Supreme Court has ruled that the First Amendment also protects the right to speak anonymously.
- Obscene speech, defamation, incitement of panic, incitement to crime, "fighting words," and sedition are not protected by the First Amendment and may be forbidden by the government.

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

- Although there are clear and convincing arguments to support freedom of speech on the Internet, the issue is complicated by the ease with which children can use the Internet to gain access to material that many parents and others feel is inappropriate for children. The conundrum is that it is difficult to restrict children's Internet access without also restricting adults' access.
- The U.S. government has passed several laws to attempt to address this issue, including the Communications Decency Act (CDA), which is aimed at protecting children from online pornography, and the Child Online Protection Act (COPA), which prohibits making harmful material available to minors via the Internet. Both laws were ultimately ruled largely unconstitutional. However, Section 230 of the CDA, which was not ruled unconstitutional, provides immunity from defamation charges to ISPs that publish user-generated content, as long as they do not also serve as a content provider.
- Software manufacturers have developed Internet filters, which are designed to block access to objectionable material through a combination of URL, keyword, and dynamic content filtering.
- The Children's Internet Protection Act (CIPA) requires federally financed schools and libraries to use filters to block computer access to any material considered harmful to minors. In *United States v. American Library Association, Inc.*, the American Library Association challenged CIPA. Ultimately in that case, the Supreme Court made it clear that the constitutionality of government-mandated filtering schemes depends on adult patrons' ability to request and receive unrestricted access to protected speech.
- The Digital Millennium Copyright Act (DMCA) addresses a number of copyright-related issues, with Title II of the act providing limitations on the liability of an ISP for copyright infringement.

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

- Internet censorship is the control or suppression of the publishing or accessing of information on the Internet. There are many forms of Internet censorship. Many countries practice some form of Internet censorship.
- A SLAPP (strategic lawsuit against public participation) is a lawsuit filed by corporations, government officials, and others against citizens and community groups who oppose them on matters of concern. Anti-SLAPP laws are designed to reduce frivolous SLAPPs. As of