FREEDOM OF EXPRESSION KEY ISSUES

Information technology has provided amazing new ways to communicate with people 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 freedom of expression, **including controlling access to information on the Internet, anonymity on the Internet, defamation and hate speech, corporate blogging, and pornography.**

Defamation

Making either an oral or a written statement of alleged fact that is false and that harms another person is defamation

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

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.

Internet Filtering

An Internet filter is software that can be used to block access to certain Web sites 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.

Internet Censorship

Internet censorship is the control or suppression of the publishing or accessing of information on the Internet. Censorship can take many forms—such as limiting access to certain Web sites, allowing access to only some content or modified content at certain Web sites, rejecting the use

of certain keywords in search engine searches, tracking and monitoring the Internet activities of individuals, and harassing or even jailing individuals for their Internet use.

Corporate Blogging

A growing number of organizations allow employees to create their own personal blogs relating to their employment. They see blogging as a new way to reach out to partners, customers, and other employees and to improve their corporate image. Under the best conditions, individual employees use their blogs to ask other employees for help with work-related problems, to share work-related information in a manner that invites conversation, or to invite others to refine or build on a new idea. However, most organizations are well aware that such blogs can also provide an outlet for uncensored commentary and interaction.

Employees can use their blogs to criticize corporate policies and decisions.

Employee blogging also involves the risk that employees might reveal company secrets or breach federal security disclosure laws.

Hate Speech

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.

Pornography

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 pornography. They are deeply troubled by its potential impact on children and fear that increasingly easy access to pornography encourages paedophiles and sexual predators.

Internet Content Rating Association (ICRA) [optional]

An Internet filter is software that can be used to block access to certain Web sites 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 Web sites. With dynamic

content filtering, each Web site's content is evaluated immediately before it is displayed, using such techniques as object analysis and image recognition

A filtering tool designed for use by Web site owners is available through ICRA (formerly the Internet Content Rating Association), which is part of the non-profit Family Online Safety Institute (FOSI),

FOSI's mission is to enable the public to make informed decisions about electronic media through the open and objective labelling of content. Its goals are to protect children from potentially harmful material while safeguarding free speech online.

In the ICRA rating system, Web authors fill out an online questionnaire to describe the content of their site. The questionnaire covers such broad topics as the presence of chat rooms or other user-generated content, the language used, nudity and sexual content, the depiction of violence, alcohol and drugs, gambling, and suicide. Within each broad category, the Web author is asked whether specific items or features are present on the site. Based on the author's responses, ICRA generates a content label (a short piece of computer code) that the author adds to the site. This label conforms to an Internet industry standard known as the Platform for Internet Content Selection (PICS). Internet users can then set their browsers to allow or disallow access to Web sites based on the information declared in the content label and their own preferences.

Note that **ICRA** does not rate Web content—the content providers do. Many hate sites and sexually explicit sites don't have ICRA ratings. Thus, these sites won't be blocked unless a browser is set to block all unrated sites, which would make Web surfing a virtually useless activity in that it would block many acceptable sites, as well. If authors lie when completing the ICRA questionnaire, their site could receive a content label that doesn't accurately reflect the site's content. For these reasons, site labelling is at best a complement to other filtering techniques.

Another approach to restricting access to Web sites is to subscribe to an Internet service provider (ISP) that performs the blocking. The blocking occurs through the ISP's server rather than via software loaded onto each user's computer. One ISP, ClearSail/Family.NET, prevents access to known Web sites that address such topics as bomb making, gambling, hacking, hate, illegal drugs, pornography, profanity, Satan, and suicide. The ISP blocks specific URLs and known pornographic hosting services, as well as other sites based on certain keywords.

IT Professional Malpractice

Negligence has been defined as not doing something that a reasonable person would do, or doing something that a reasonable person would not do. Duty of care refers to the obligation to protect people against any unreasonable harm or risk. For example, people have a duty to keep their pets from attacking others and to operate their cars safely.

If a court finds that a defendant actually owed a duty of care, it must determine whether the duty was breached. A breach of the duty of care is the failure to act as a reasonable person would act. A breach of duty may consist of an action, such as throwing a lit cigarette into a fireworks factory and causing an explosion, or a failure to act when there is a duty to do so—for example, a police officer not protecting a citizen from an attacker.

Courts have consistently rejected attempts to sue individual parties for computer-related malpractice. Professional negligence can only occur when people fail to perform within the standards of their profession, and software engineering is not a uniformly licensed profession in the United States**. Because there are no uniform standards against which to compare a software engineer's professional behaviour, he or she cannot be subject to malpractice lawsuits.**

John Doe Lawsuits

Businesses must protect against both the public expression of opinions that might hurt their reputations and the public sharing of company confidential 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 Internet service provider or a Web site 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).

A company may file a John Doe lawsuit because it is upset by anonymous e-mail messages that criticize the company or reveal company secrets.

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.

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 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 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.

CONTINGENTWORKERS

The Bureau of Labor Statistics defines contingent work as a job situation in which an individual does not have an explicit or implicit contract for long-term employment. The contingent workforce includes independent contractors, temporary workers hired through employment agencies, on-call or day laborers, and on-site workers whose services are provided by contract firms.
A firm is likely to use contingent IT workers if it experiences pronounced fluctuations in its technical staffing needs. Workers are often hired on a contingent basis as consultants on an organizational restructuring project, as technical experts on a product development team, and as supplemental staff for many other short-term projects, such as the design and installation of new information systems.