Ethics in Information Technology

Freedom of Expression

Objectives

- As you read this chapter, consider the following questions:
  - What is the basis for the protection of freedom of expression in the United States, and what types of expression are not protected under the law?
  - What are some key federal laws that affect online freedom of expression, and how do they impact organizations?
  - What important freedom of expression issues relate to the use of information technology?

Freedom of Expression and Internet

- Internet Enables
  - News – ideas-rumors-information
  - Open discussions – anonymity
- Ethical use of this freedom and power
- Government and organizations have made laws and policies to guide people in this and protect their own interest
- Right of freedom of expression
- First amendment guarantee this right
- Several federal/state laws found unconstitutional

First Amendment Rights

- Definition of free speech includes:
  - Nonverbal, visual, and symbolic forms of expression
  - Right to speak anonymously
  - A speech highly unpopular for majority – protection of minority views

First Amendment Rights (cont'd.)

- Not protected by the First Amendment
  - Perjury
  - Fraud
  - Defamation
  - Obscene speech
  - Incitement of panic
  - Incitement to crime
  - "Fighting words"
  - Sedition
- Obscene speech and Defamation relevant to IT

Obscene Speech

- Based on *Miller v. California*, speech is considered obscene when:
  - Lacks serious literary, artistic, political, or scientific value

Defamation

- Oral or written statement of alleged fact that is:
  - False
  - Harms another person
    - Harm is often of a financial nature
- Slander
  - Oral defamatory statement
- Libel
  - Written defamatory statement
- Care in online communication to avoid charges of defamation
- Organizations prepared to take actions against libelous attacks

Freedom of Expression: Key Issues

- Controlling access to information on the Internet
- Anonymity on the Internet
- Defamation and hate speech
- Corporate blogging
- Pornography

Controlling Access to Information on the Internet

- Freedom of speech on the Internet is complicated by ease by which children can access Internet
- Laws and software to block questionable material
- Communications Decency Act (CDA 1996)
  - Aimed at protecting children from pornography
  - Broad language and vague definition of indecency
  - Found unconstitutional in 1997

Controlling Access to Information on the Internet (cont'd.)

- Child Online Protection Act (COPA 1998)
  - Applies to communication for commercial purposes
  - Imposes penalties for exposing minors to harmful material on the Web
  - Found unconstitutional in 2004
- Internet filtering
  - Software installed with a Web browser
  - Blocks access to certain Web sites deemed to contain inappropriate or offensive material

FIGURE 5-3 Screenshot of Safe Eyes® from Internet Safety

Source Line: Used with permission from InternetSafety.com, part of McAfee Inc.

Controlling Access to Information on the Internet (cont'd.)

- URL filtering
  - Blocks objectionable URLs or domain names
- Keyword filtering
  - Blocks keywords or phrases
- Dynamic content filtering
  - Web site's content is evaluated immediately before being displayed
  - Uses
    - Object analysis
    - Image recognition

Controlling Access to Information on the Internet (cont'd.)

- Top-rated Internet filters for home users
  - NetNanny Parental Controls
  - PureSight PC
  - CYBERsitter
  - SafeEyes
  - CyberPatrol

Controlling Access to Information on the Internet (cont'd.)

- ICRA rating system
  - Questionnaire for Web authors
  - Generates a content label
    - Platform for Internet Content Selection (PICS)
  - Users configure browsers to read the label
  - Relies on Web authors to rate their site
  - Complement to other filtering techniques

Controlling Access to Information on the Internet (cont'd.)

- ISP blocking
  - Blocking is performed on the ISP server
  - ClearSail/Family.NET prevents access to certain Web sites
  - List is updated

Children's Internet Protection Act (CIPA)

- Federally financed schools and libraries must block computer access to:
  - Obscene material
  - Pornography
  - Anything considered harmful to minors

Children's Internet Protection Act (CIPA)

- Schools and libraries subject to CIPA do not receive Internet access discounts unless they:
  - Put in place measures to filter pictures that are obscene, or are harmful to minors
  - Adopt a policy to monitor the online activities of minors
  - Adopt a policy restricting minors' access to materials harmful to them

Children's Internet Protection Act (CIPA) (cont'd.)

- CIPA does not require the tracking of Internet use by minors or adults
- Acceptable use policy agreement is an essential element of a successful program in schools
  - Signed by:
    - Students
    - Parents
    - Employees

Children's Internet Protection Act (CIPA) (cont'd.)

- Difficulty implementing CIPA in libraries because their services are open to people of all ages
  - Including adults with First Amendment rights
- CIPA has been upheld as constitutional by U.S. Supreme Court (*U.S. v American Library Association*)

Anonymity on the Internet

- Anonymous expression is expression of opinions by people who do not reveal their identity
- Freedom to express an opinion without fear of reprisal is an important right in democratic society
- Anonymity is even more important in countries that do not allow free speech
- Played important role in early formation of U.S.
- In the wrong hands, it can be a tool to commit illegal or unethical activities

Anonymity on the Internet

- 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
- **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**

Anonymity on the Internet

- 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,
  - 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

Anonymity on the Internet (cont'd.)

- Anonymity is important for internet users – they maybe
  - Seeking help in online support groups
  - Reporting defects in manufacturer product
  - Taking part in sensitive discussion
- Others oppose
  - Defamation
  - Fraud
  - Libel
  - Exploitation of children

Anonymity on the Internet (cont'd.)

- Anonymous remailer service
  - Computer program that strips the originating address from the email message
  - Forwards the message to the intended recipient
  - Ensures no header information can identify the author
  - Keeps what is communicated anonymous
  - What is communicated and whether it is ethical or unethical, legal or illegal, is up to the sender

Anonymity on the Internet (cont'd.)

- Anonymous remailer service
  - 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

Anonymity on the Internet (cont'd.)

- John Doe lawsuit
  - Business must protect against
    - Public sharing of opinion that hurt its reputation
    - Public sharing of confidential information
    - Hard to identify person
  - John Doe lawsuit can be filed against anonymous
  - Court can summon to appear in court
  - By court permission, plaintiff can serve subpoenas
    - ISP
    - Web site hosting firm

Anonymity on the Internet (cont'd.)

- John Doe lawsuit
  - Defendant communicates anonymously so identity of defendant is temporarily unknown
  - Common in Internet libel cases
  - the plaintiff can request court permission to issue subpoenas to command a person to appear under penalty
  - If court permission, plaintiff can serve subpoenas to third party
  - Few examples to follow

Anonymity on the Internet (cont'd.)

- John Doe lawsuit
  - For example, Raytheon filed a lawsuit in 1999 for $25,000 in damages against 21 John Does for allegedly revealing on a Yahoo! message board company financial results along with other information that the company claimed hurt its reputation. Raytheon received a court order to subpoena Yahoo! and several ISPs for the identity of the 21 unnamed defendants. Eventually, Raytheon traced the identities of all 21 people who posted the alleged company secrets. Four employees voluntarily left the company, and others received counseling about sharing confidential company information.

Anonymity on the Internet (cont'd.)

- John Doe lawsuit
  - America Online, Verizon Online etc receive more than 1000 subpoenas per year
  - Free speech advocates that if someone charges libel, their identity should be hidden until proved
  - stock price manipulators can use chat rooms to affect the share price of stocks
  - competitors of an organization might try to create the feeling that organization is a miserable place to work

Anonymity on the Internet (cont'd.)

- John Doe lawsuit
  - The California State Court in Pre-Paid Legal v.Sturtz et al. set another legal precedent that refined the criteria that 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 Pre-Paid message board. Attorneys for PPLS argued that it 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. ……

Anonymity on the Internet (cont'd.)

- John Doe lawsuit
  - The Electronic Frontier Foundation (EFF) represented two John Does. EEF argued that they just criticized the company and their treatment with sales person. And they did not reveal any trade secrets. Also the company may punish them and set precedent for others to not to criticize. EEF urged the court to apply four-part test.

Anonymity on the Internet (cont'd.)

- John Doe lawsuit
  - Subpoena should be enforced only when
    - 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.
  - August 2001, a judge in Santa Clara County Superior Court invalidated the subpoena to Yahoo! requesting the posters' identities

Defamation and Hate Speech

- Hate speech that can be prosecuted includes:
  - Clear threats and intimidation against specific citizens
  - Sending threatening private messages over the Internet to a person
  - Displaying public messages on a Web site describing intent to commit acts of hate-motivated violence against specific individuals
  - Libel directed at a particular person

Defamation and Hate Speech (cont'd.)

- annoying, critical, offensive speech protected
- Legal liability when
  - Threats
  - Intimidation against specific person
- ISPs reserve the right to remove data that is not up to their standards
- AOL set of standards guidelines
  - Not responsible for delay or failure in removing
  - AOL has right to enforce them

Defamation and Hate Speech (cont'd.)

- Such actions do not violate the subscriber's First Amendment rights because these prohibitions are in the terms of service
  - ISPs must monitor the use of their service
  - Take action when terms are violated

Defamation and Hate Speech (cont'd.)

- Public schools and universities are legally considered agents of the government and must follow the First Amendment prohibition against speech restrictions
- Corporations, private schools, and private universities not part of state or federal government
  - May prohibit students, instructors, and employees from engaging in offensive speech
- Example to follow

Defamation and Hate Speech (cont'd.)

- Former student was sentenced to one year in prison for sending e-mail death threats to Asian American students at the University of California, Irvine. His e-mail was signed "Asian hater," and his letters stated that he would make it his career to find and kill every Asian himself.

Defamation and Hate Speech (cont'd.)

- Many countries don't provide protection for hate speech
  - Promoting NAZI ideology is crime in Germany
  - Denying holocaust is illegal in European Countries
- **Thousands of people faced the potential of criminal charges after posting hate messages and threats to the Facebook account of Brendan Sokaluk, who is accused of setting bushfires that killed 21 people in Victoria, Australia, in February 2009. "It's the cyber-world equivalent of angry mobs forming outside court, hurling abuse," said Michael Pearce**

Defamation and Hate Speech (cont'd.)

- Across the borders
  - A U.S. citizen who posts material on the Web that is illegal in a foreign country can be prosecuted if he subjects himself to the jurisdiction of that country
  - He is safe in U.S
  - laws do not allow a person to be extradited for engaging in an activity protected by the U.S.
  - Even if the activity violates the criminal laws of another country

Corporate Blogging

- Some organizations allow employees to create their own personal blogs to:
  - Reach out to partners, customers, and employees
  - Improve their corporate image
  - Discuss work-related issues
  - Invite others to refine or build new idea
- Blogs can provide uncensored commentary and interaction
  - Criticism of corporate policies and decisions

Corporate Blogging

- Could involve risk that employees might:
  - Reveal company secrets
  - Breach federal security disclosure laws
- Guidelines
  - Don’t reveal company secrets
  - Make it appealing
  - Be interesting
  - Be authentic

Corporate Blogging

- Mark Jen, an associate product manager for Google, began a blog chronicling his experiences at Google after his first day on the job. He thought his entries might be of interest to his family and friends. His entries candidly discussed his first day on the job, a global sales meeting, and Google's compensation package. His comments also included information about Google's future products and economic performance. Within a couple of days, Mark's audience had grown into the tens of thousands.

Corporate Blogging

- The following week, Mark's blog was offline for a couple days. In his next posting, Mark revealed that he had been asked to take down sensitive information about the company. Then the entries stopped altogether, and rumors were rampant as the number of visitors to his blog approached 100,000 per day. A few weeks later, Mark finally checked back in to let his readers know that he had been fired. Within the blogosphere, Mark had become a cause célèbre, and Google's reputation suffered. The incident sent a shock wave through the IT industry, forcing companies to evaluate and establish their own blogging policies.

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 non-business use of information resources?		
Did the developers of your policy consider the need to limit employee access to non-business-related Web sites (for example, 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 e-mail?		
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 or sending of pornography?		
Does your policy communicate if employee e-mail 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?		

Summary

- First Amendment protects the right to:
  - Freedom of religion and expression
- Does not protect obscene speech, defamation
- Key issues
  - Controlling access to Internet information, especially for children
  - Anonymous communication
  - Spread of defamation and hate speech
  - Access to pornography
  - CAN-SPAM Act limitations on email messages