

# Chapter 4: Freedom of Speech

# Freedom of Speech

- Includes speech of everyone, including controversial or offensive ideas.
- Does not entitle speakers to agreement from others or even others' attention.
- Media and press are an extension of free speech of the people.
- Valued differently in different societies.

# Themes

---

- First Amendment
- Censorship
- Digital Media & Free Speech
- Leaking & Whistle-blowing
- Net Neutrality

# First Amendment

*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.*

# First Amendment

- Written for unpopular, offensive, and/or controversial speech and ideas.
- Covers spoken and written words, pictures, art, and other forms of expression of ideas and opinions.
- Restriction on the power of government, not individuals or private businesses.

# Free Speech Principles

- Advocating illegal acts is (usually) legal.
  - Inciting an imminent criminal act is not legal.
- Anonymous speech is protected.
- Some restrictions allowed on advertising.
- Libel, specific threats, and obscenity are not protected.

# Free Speech Guidelines

- Distinguish speech from action.
- Laws must not reduce expressiveness of legal speech.
- Do not reduce adults to only what is fit for children.
- Solve problems by least restrictive means.

# Obscenity

- Depicts a sexual act that is against the law.
- Depicts these acts in a patently offensive manner that appeals to prurient interest as judged by a reasonable person using community standards.
- Lacks literary, artistic, social, political or scientific value.

# Internet Censorship Laws

Communications Decency Act of 1996  
(CDA):

- Attempted to avoid conflict with First Amendment by focusing on children.
- Made it a crime to make available to anyone under 18 any obscene or indecent communication.

# Internet Censorship Laws

Communications Decency Act of 1996  
(CDA):

- Found to be unconstitutional:
  - The worst material threatening children was already illegal.
  - It was too vague and broad.
  - It did not use the least restrictive means of accomplishing the goal of protecting children.

# Internet Censorship Laws

Child Online Protection Act of 1998  
(COPA):

- More limited than CDA.
- Federal crime for commercial Web sites to make available to minors material “harmful to minors” as judged by community standards.

# Internet Censorship Laws

Child Online Protection Act of 1998  
(COPA):

- Found to be unconstitutional
  - It was too broad.
  - It would restrict the entire country to the standards of the most conservative community.
  - It would have an impact on the expressiveness of speech.

# Internet Censorship Laws

---

Children's Internet Protection Act of  
2000 (CIPA):

- Requires schools and libraries that participate in certain federal programs to install filtering software.

# Internet Censorship Laws

Children's Internet Protection Act of  
2000 (CIPA):

- Upheld in court
  - Does not violate First Amendment since it does not require the use of filters by non-government groups, impose jail or fines.
  - Sets a condition for receipt of certain federal funds.

# Alternatives to Censorship

- Content filters
  - Blocks sites with specific words, phrases or images
  - Parental control for sex and violence
  - Updated frequently but may still screen out too much or too little
  - Not possible to eliminate all errors
  - What should be blocked?

# Alternatives to Censorship

- Policies
  - Commercial services, online communities, and social networking sites develop policies to protect members.
  - Video game industry developed rating system that provides an indication for parents about the amount of sex, profanity, and violence in a game.

# Free Speech Online

Speech on the Internet requires several parties:

- Hosts
- Search engines
- Domain Name System
- Internet service providers

# Hosts

- Owners of systems that host your web content.
- Often first to be given takedown notices or have complaints reported.
- Have motivation to keep positive relationship with government agencies.
- May have their own policies about kinds of speech allowed or may censor criticism of themselves.

# Search Engines

- One of the most common ways to connect users to new content.
- Another target for takedown notices and complaint reporting.
- Often not allowed to operate in country if they don't censor according to local criteria.
- Sometimes pressured by content providers in order to be able to index their content.

# Domain Name System

- Translate domain names into IP addresses.
- If content's domain name is de-listed, users may be unable to find address for connecting to content.
- When a domain is de-listed, impacts both legal and illegal content on that domain.
- Domain provider in U.S. de-listed Wikileaks after releasing U.S. embassy communications.

# Internet Service Providers

- Provide users' connection to the Internet.
- When user's IP is traced, leads back to ISP.
- Must balance legal liability with income from particular users.
- May shut down users' connections after set number of complaints.
- Protected by U.S. law, but only if they comply with guidelines for complaints from government and copyright holders.

# Leaking & Whistle-Blowing

***leaking***: disclosing secret, official information to the media or public, often anonymously.

**whistle-blowing**: exposing information about activities which may be illegal, unethical, or immoral within an organization.

# Leaking & Whistle-Blowing

Considerations about leaked material:

- Type of material.
- Value to society.
- Risk to society or individuals.

# Leaking & Whistle-Blowing

- Software vulnerabilities
- Military misdeeds
- Covert actions by governments
- Illegal or corrupt business practices
- Discrimination

# Leaking & Whistle-Blowing

Examples:

- Chelsea Manning (Iraq War documents)
- Edward Snowden (NSA surveillance)
- Climategate (U.K. scientists reveal falsified climate data)

# Leaking & Whistle-Blowing

Responsibilities of hosts for leaked information:

- Verifying information.
- Protecting identity of source.
- Vetting data to remove details that could endanger people.
  - Especially hard for large collections.

# Leaking & Whistle-Blowing

- Occupational Safety & Health Act of 1970 protects whistle-blowers from retaliation by employers.
- Whistleblower Protection Act of 1989 protects federal whistleblowers who work for the government and report agency misconduct.
- Espionage Act of 1917 is increasingly used against federal employees who release information publicly.

# Net Neutrality

***net neutrality***: the principle that Internet service providers should enable access to all content and applications regardless of the source, and without favoring or blocking particular products or websites.

# Net Neutrality

- In 2005, a local broadband company blocked VoIP to promote their own services.
  - FCC ordered them to un-block.
- In 2007, Skype asked FCC to do the same for mobile broadband, but was not granted.
- In 2008, Comcast blocked Bittorrent traffic.
  - FCC ordered them to un-block.
- In 2014, Netflix paid Comcast for higher priority on their network.

# Net Neutrality

Arguments for neutrality:

- Internet was designed for equal access.
- Multiple “lanes” would create a tiered society online.
  - Harmful to innovation.
- ISPs can abuse their control.
- Blocking things like Bittorrent removes legitimate uses.

# Net Neutrality

Arguments against neutrality:

- Limits adaptability for ISPs.
- Some services have more social and economic value than others.
- Market can solve problems.
- Higher volume services should be “paying their own way.”

# Net Neutrality

- In 2015, FCC issued “Open Internet Rules”
  - No paid prioritization.
  - No blocking services for legal content.
  - No slowing down access to legal content.