CSE/ISE 312

Freedom of Speech (Part 2)

“Anonymity is a shield from the tyranny of the majority”
- US Supreme Court

Posting, Selling, Leaking Sensitive Material

- There are social and ethical issues on publication and distribution of legal material that is sensitive
  - Hoaxes, legal adult entertainment, vicious personal attacks by bloggers, info on how to make bombs
- Do web sites/search engines have a social, ethical obligation for complete content/search results?
  - Web companies face difficult questions when setting policies
- Individuals should use discretion when posting

Posting Sensitive Material

- Policies of large companies

  Do search engine providers have a social or ethical obligation to provide complete search results to all queries, or do they have a social or ethical obligation to omit very offensive sites from search results?

- A Web site with risks

  People should consider potential risks of posting material. They should consider unintended readers or users and should consider ways to prevent access by unintended users.

Leaking Sensitive Material

- Leaks
  - Type of material
  - Value to society
  - Risks to society and individuals

- The Web is a convenient and powerful tool for whistle blowers. Some leaks serve valuable social purposes

Leaking: Right or Wrong?

- We should remember that leaking begins with a strong ethical case against it
  - Freedom of speech and press do not legitimate stealing files and publishing them
  - This does not mean that leaking is always wrong
  - It means that the reasons for leaking the material must be strong enough to overcome the ethical arguments against it, and the publisher of the leaked material must handle it responsibly
- Documents that include significant evidence of serious wrongdoing are reasonable candidates for leaks

Leaking Sensitive Material - Examples

- WikiLeaks

  released U.S. military documents related to the wars in Iraq and Afghanistan, including videos of shooting incidents; confidential U.S. diplomatic cables

- Climategate:

  leaked emails show that researchers at the University of East Anglia pursued a variety of methods to deny access to their temperature data by scientists who question some aspects of global warming

Potentially Dangerous Leaks

- WikiLeaks released a secret U.S. government cable listing critical sites, such as telecommunications hubs, dams, pipelines, supplies of critical minerals, manufacturing complexes, and so on, where damage or disruption would cause significant harm

- Some cables named whistleblowers, confidential informants, human rights activities, intelligence officers. These put those people at risk

Releasing a Large Mass of Documents

- WikiLeaks made public ~250,000 diplomatic cables of the US government and thousands of other documents
- Climategate leaks included thousands of documents
- Did the leakers review and evaluate all the documents they released to be sure they met reasonable criteria to justify the leaks? Should they have?

Responsibilities of operators of Web sites for leaks

- A person or organization establishing a site to publish leaked documents that serve an important public purpose should consider the various points already raised, but also has responsibilities to avoid abuse of the site
- The site must have sufficient security to protect whistleblowers
- A well-thought-out policy about how to handle requests or demands from law enforcement agencies
- Verification of the authenticity and validity of leaked documents

Guidelines on Posting Sensitive Materials

- Consider unintended readers or users
- Consider potential risks
- Consider ways to limit access to intended users
- Remember it is difficult to remove material from the Net once you have posted it

Anonymity

- Historical precedent for anonymous publication
  - Thomas Paine's name did not appear on the first printings of *Common Sense*, the book that roused support for the American Revolution.
  - The Federalist Papers, published in newspapers in 1787 and 1788, argued for adoption of the U.S. Constitution. The authors, Alexander Hamilton, James Madison, and John Jay, used the pseudonym, Publius.

Positive Uses of Anonymity

- Protecting privacy, against identity theft/profiling
- Protect political speech
- Protect against retaliation and embarrassment
- Company new products development

- Anonymizing services
  - Services available to send anonymous email (Anonymizer.com)
  - used by individuals, businesses, law enforcement agencies, and government intelligence services

Anonymizer Technology

- Use proxies (either single point or networked)
  - E.g., one remailer, or many intermediate remailers
  - May allow two-way anonymous communications
- Usually encrypts user/browser communication
- Proxy removes any identifying information from transmission to server
- Product offered at anonymizer.com

Negative Uses of Anonymity

- hides crime, protects criminal and antisocial activities
- aids fraud, harassment, extortion, libel, distribution of child pornography, theft, and copyright infringement
- masks illegal surveillance by government agencies
- glowing reviews (such as those posted on eBay or Amazon.com) may actually be from the author, publisher, seller, or their friends

The First Amendment

- Anonymity protected by the First Amendment

- “Anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority” – Supreme court, 1995

Is Anonymity Protected?

- Many legal issues about anonymity are similar to those discussed in Chapter 2
- Should ISPs be required to notify a member when the ISP receives a subpoena for the member's identity, so the person has an opportunity to fight a subpoena in court?
- Does the potential for harm by criminals who use anonymity to hide from law enforcement outweigh the loss of privacy and restraint on freedom of speech for honest people who use anonymity responsibly?

SLAPP

- SLAPP (Strategic Lawsuit Against Public Participation)

  A SLAPP is a lawsuit filed (generally libel) intended to censor/intimidate/silence critics by burdening them with the cost of a legal defense. Identities of critics obtained via subpoena
- At least 26 states have enacted anti-SLAPP laws
  - Allows subject to file a motion
  - If granted, motion reduces legal requirements of defendant and awards legal fees to defendant
- Issue of action when an ISP receives a subpoena for the identity of an “anonymous” user

Laws against Anonymity

- U.S. and European countries working on laws that require ISPs to maintain records of the true identity of each user and maintain records of online activity for potential use in criminal investigations

- Does the potential for harm by criminals who use anonymity to hide outweigh the loss of privacy and restraint on freedom of speech for honest people who use anonymity responsibly?
- Is anonymity an important protection against possible abuse of government power?