312 Test Review 1

Ethics,

Privacy,

Freedom of Speech,

Intellectual Property

Ethical Views (1)

Deontological (nonconsequentialist) theories

- View acts as good or bad based on the intrinsic aspect of the action. Emphasize duty, absolute rules (e.g., do not lie)
- Three Immanuel Kant's ideas about ethics:
  - Principle of universality: we should follow rules of behavior that we can universally apply to everyone
  - Logic and reason determines rules of ethical behavior. One should use reason, rationality, and judgment, not emotions, when making ethical decisions
  - Never treat people as merely means to ends, but rather as ends in themselves

Ethical Views (2)

Utilitarianism (a consequentialist theory)

- Consider consequences, aim to increase happiness, or net aggregate utility;
  - Utility: what satisfies a person's needs and values
  - Aggregate utility: consider all affected people
- an act is right if it increases aggregate utility
- Distinguish act utilitarianism and rule utilitarianism
  - Act: Consider utility of each act
  - Rule: Consider utility of general ethic rules instead, not individual act

Ethical Views (3)

Natural rights

Try let people make their own decisions, act freely according to their own judgment

- Ethical behaviors respect fundamental/natural rights including rights to life, liberty, and property
- Acts are likely ethical if they involve voluntary interactions and freely made exchanges, where the parties are not coerced or deceived
  - Emphasize the process by which people interact, not the result of the interaction

Negative rights vs. Positive rights

- Negative rights (liberties)
  - The rights to act without interference
- Positive rights (claim-rights)
  - An obligation of some people to provide certain things for others, such as work, food, medical care, etc.
- Negative rights and positive rights often conflict
  - Some think protecting claim rights is essential, some think protecting liberties is essential

Negative rights vs. Positive rights

- Negative rights (liberties)
  - Right to life, liberty, and the pursuit of happiness
  - Right to freedom of speech and religion
  - Right to work, own property, access the Internet
- Positive rights (claim-rights)
  - To life: someone is obligated to pay for food/medical care
  - To freedom of speech
  - To a job: someone must hire you
  - To access Internet: subsidized access for poor people

Privacy Risks and Principles

Three Key Aspects of Privacy:

- Freedom from intrusion - being left alone
- Control of information about oneself
- Freedom from surveillance (from being tracked, followed, watched, eavesdropped on)

Definitions

- Personal information – any information relating to, or traceable to, an individual person
- Informed consent – users being aware of what information is collected and how it is stored
- Invisible information gathering - collection of personal information about someone without the person's knowledge
- Cookies - files that a website stores on a visitor's computer

Summary of Privacy Issues (1)

- Almost everything we do online is recorded
- Huge amounts of data are stored
- People are often not aware of collection of personal data
- Software is complex, not even sure which collects data
- Leaks happen
- A collection of many small data items can provide a detailed picture of person's life

Summary of Privacy Issues (2)

- **Re-identification** – piecing together someone's identity - has become much easier than before
- Information available on the Internet will be found by people for whom it was not intended
- Electronic data seems to last forever
- Data collected for one purpose will find other uses
- The government sometimes requests personal data
- We cannot directly protect information about ourselves

Terminology

- Secondary use - use of personal information for a purpose other than the one it was provided for
- Data mining - searching and analyzing masses of data to find patterns and develop new information or knowledge
- Computer matching - combining and comparing information from different databases (using social security number, for example) to match records
- Computer profiling - analyzing data in computer files to determine characteristics of people most likely to engage in a certain behavior

Principles for Data Collection and Use

- Informed consent – informing people how collected information is being used
- Opt-in and opt-out policies – people specify an exception to the default condition (either to not use information or use information by default)
- Data retention - is the continued storage of an organization's data for compliance or business reasons.
  - An organization may retain data for several different reasons. One reason is to comply with state and federal regulations. Another is to provide the organization with the ability to recover business critical data in the event of a site-wide data loss, such as a fire or flood.

Forms of Informed Consent

Two common forms for providing informed consent are opt in and opt out:

- opt in – The collector of the information may use information only if person explicitly permits use (usually by checking a box)
- opt out – Person must request (usually by checking a box) that an organization *not* use information

Fair Information Principles (FIP)

- Recommendations from privacy experts
  1. Inform people when you collection information, what you collect and how you use it
  2. Collect only the data needed
  3. Offer opt-outs
  4. Keep data only as long as needed
  5. Maintain accuracy of data
  6. Protect security of data
  7. Develop policies for law enforcement requests

The Fourth Amendment

- Part of the US Bill of Rights
- ***"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."***

Supreme Court Decisions and Expectation of Privacy (1)

- Supreme court decisions continue to address impact of new tech on 4th Amendment protection
- *Olmstead v. United States* (1928)
  - Supreme Court allowed the use of wiretaps on telephone lines without a court order
  - Interpreted the Fourth Amendment to apply only to physical intrusion and only to the search or seizure of material things, not conversations.

Supreme Court Decisions and Expectation of Privacy (2)

- *Katz v United States* (1967)
  - Supreme Court reversed its position and ruled that the Fourth Amendment *does* apply to conversations
  - Court said that the Fourth Amendment protects people, not places. To intrude in a place where reasonable person has a reasonable expectation of privacy requires a court order

Supreme Court Decisions and Expectation of Privacy (3)

- *Kylo v United States* (2001)
  - Supreme Court ruled that police could not use thermal-imaging devices to search a home from the outside without a search warrant.
  - Court stated that where "government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search.'"

A Right to Be Forgotten

- The right to have material removed
- US and EU are promoting such a legal right
- Many practical, ethical, social, legal questions arise
- negative right (a liberty)
- positive right (a claim right)
- Possible conflict with free speech, free flow of information, and contractual agreements

Privacy Act of 1974

"No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains... except"

- For statistical purposes by the Census
- For routine uses within a U.S. government agency
- For archival and law enforcement purposes
- For congressional investigations and other admin purposes

Government Databases

Government Accountability Office (GAO)

- Congress' agency to monitor government's privacy policies, and enforces the Act
- Has noted numerous variations from the law; they do not adequately protect our data
- Rules for government use of commercial databases, or commercial search engine results are vague or missing

Case studies: College student database, data mining and computer matching to fight terrorism

Public Record Data

- Public Records - records available to general public (bankruptcy, property, arrest records, salaries of government employees, etc.)
- Governed by the Freedom of Information Act (FOIA): rules on access to records held by government bodies
  - Basic principle – burden of proof falls on the body asked for information (not requester)
  - Act applies to federal agencies, but states have similar laws
  - Includes electronic access (1996)
- Electronic access creates new privacy issues

National ID System

- Social Security Numbers
  - Increasingly used as a national ID from 1936-1980s
  - Easy to falsify/inadvertently disclose, fraud/id theft
- A new national ID system - Pros
  - would require the card
  - have to carry only one card
  - Reduce fraud, illegal workers, terrorists
- A new national ID system - Cons
  - Threat to freedom and privacy
  - Large amount data on it increase potential for abuse

Encryption

- “Cryptography is the art and science of hiding data in plain sight”
- Used to protect data in transit and also stored information
- Includes a cryptographic algorithm, and keys. A very simple one: a scrambled alphabet
- Usually the longer the key, the more difficult to break the cipher
- Government ban on export of strong encryption software in the 1990s (removed in 2000)

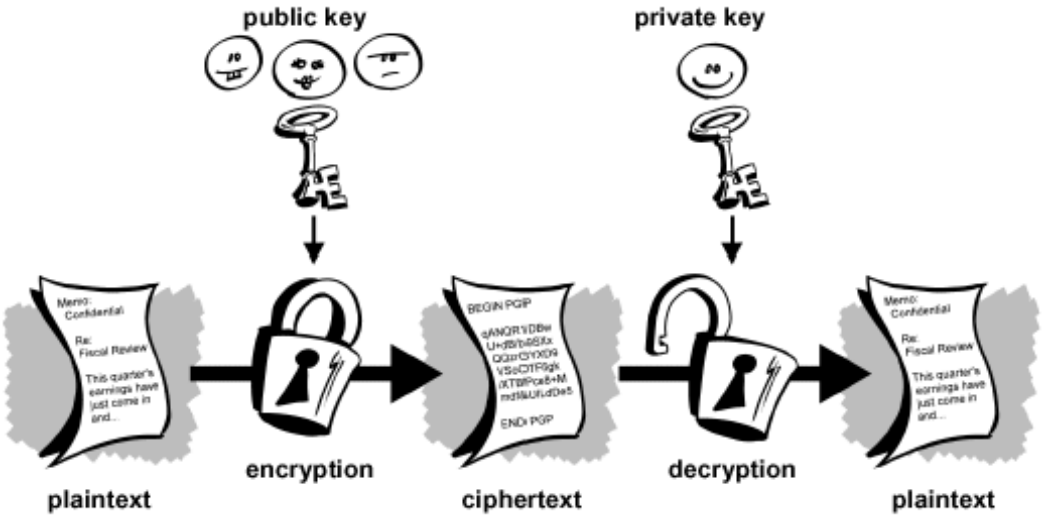
Public-Key Encryption (PKE) (1)

- Keys are secret information that is critical to the security/success of the scheme. Can be numbers, strings, etc.
- In PKE, keys come in a pair:
  - one is made public to the world, called public key
  - one is kept only to oneself, called private key
- To provides "confidentiality", i.e., only B can see the content of a received message
  - A sender encrypts with B's public key and sends it
  - B decrypts with B's private key

Public Key Encryption (2)

- To provide "authentication", we say entity A signs a document
  - To do so, A encrypts with A's private key and sends it
  - The receiver decrypts with A's public key to verify

confidentiality



Wiretapping and E-Mail Protection

- Telephone
  - 1934 Communications Act prohibited interception of messages that is not authorized by the sender
  - 1968 Omnibus Crime Control and Safe Streets Act allowed wiretapping and electronic surveillance by law-enforcement (with court order)
- E-mail and other new communications
  - Electronic Communications Privacy Act of 1986 (ECPA) extended the 1968 wiretapping laws to include electronic communications, restricts government access to e-mail
  - Patriot Act loosens restrictions on government surveillance and wiretapping

Designing for Interception

- Communications Assistance for Law Enforcement Act of 1994 (CALEA)
  - Telecommunications equipment must be designed to ensure government can intercept telephone calls (with a court order or other authorization)
  - Rules and requirements written by Federal Communications Commission (FCC), which ruled that CALEA requirements extend to new services (cell phones and Internet phones)
  - Arguments in favor and against CALEA

Secret Intelligence Gathering

- The National Security Agency (NSA)
  - Collects and analyzes foreign intelligence data related to national security
  - Protects US Government communications
  - Prohibited from intercepting communications within the US
- Foreign Intelligence Surveillance Act (FISA) established oversight rules for the NSA
- Secret access to communications records

First Amendment, U.S. Constitution

- "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."

3-Part Framework for Protection

Print media

Broadcast (tv,radio)

Common carriers
(phone, postal svc)

Telecommunication Act of 1996

- Major overhaul of telecommunications law
- Changed regulatory structure, removed artificial legal divisions of service areas and restrictions on telephone companies' services
- "No provider or user of interactive computer service shall be treated as a publisher of any information provided by another information content provider"
- Title V of the Act is Communications Decency Act (CDA) outlines regulations concerning obscene materials
  - First major Internet censorship law.

Free-Speech Principles

- Supreme Court principles and guidelines
  - Laws must not chill expression of legal speech
    - "Chilling effect" laws are generally unconstitutional
  - Distinguish speech from action. Advocating illegal acts is usually legal
  - Does not protect libel and direct, specific threats
  - Inciting violence, in certain circumstances, is illegal
  - Allow some restrictions on advertising*
  - Protect anonymous speech*

Obscenity

- Supreme Court guidelines (1973) rule that obscenity
  - Depicts a sexual act against state law,
  - Depicts these acts in a patently offensive manner that appeals to prurient interest as judged by a reasonable person using community standards, and
  - Lacks literary, artistic, social, political or scientific value

Obscenity

- Internet changes practicality of community standard principle – want to restrict the country to the standard of the most conservative community?

Communication Decency Act (CDA)

- Attempted to outlaw indecent communications by focusing on children
  - made it a crime to make available to anyone under 18 any communication that is obscene or indecent
- Found to be unconstitutional: (1997)
  - Too vague and broad, filtering is less restrictive

Communication Decency Act (CDA)

- More free speech guidelines
  - Solve speech problems by least restrictive means
  - Do not reduce adults to reading only what fits children
- Court ruled that the Internet "deserves the highest protection from government intrusion

Child Online Protection Act (COPA)

- Another Internet censorship law
- It would be a federal crime for commercial web sites to make available to minors harmful material as judged by community standards (1998)
- Found to be unconstitutional: (2000)
  - Community standard is too restrict
  - Restricts access to lawful content for adults
  - Chilling effect

Children's Internet Protection Act (CIPA)

- Enacted in 2000
- Requires schools and libraries that participate in certain federal programs to install filtering software. Can disable the filter for adults.
- Upheld in court: (2003)
  - Does not violate First Amendment since it does not require the use of filters,
  - Does not impose jail or fines on people who provide content on the Internet,
  - It sets a condition for receipt of certain federal funds

Video Games & Alternatives to Censorship

- Violent video games for children
  - Are they more dangerous than other forms that a minor sees in books or other media?
  - In 2011, Supreme Court ruled that violence is common is classic fairy tales, etc. Disgust is not a valid basis for restricting expression. Research found that the impact was small and differed little from the impact of other media
- Alternatives to censorship
  - Wireless carriers' stricter rules on decency
  - Policies that expel subscribers who post illegal, offensive materials, e.g. child pornography
  - Video rating of sex, profanity, and violence

Spam

- Unsolicited bulk email, text, tweets, calls, etc
- Free speech issues
  - Spam imposes a cost on others not protected by free speech
  - Spam filters do not violate free speech (free speech does not require anyone to listen)
- Anti-spam Laws
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act), federal, 2004
  - Targets commercial spam. Require valid headers, id info. etc.
  - Criticized for not banning all spam, legitimized commercial spam

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?

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

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

Net Neutrality Regulations or the Market?

- *Common carriers* were prohibited from providing own content, and from discrimination based on content or source, called line-sharing (open-access) requirements
- It was argued that line-sharing/inflexible prices reduced incentive for investment to improve broadband capacity and innovation
  - FCC eliminated line-sharing requirements (2003-2005)

 Net Neutrality refers to a variety of proposals for restrictions on how telephone and cable companies interact with their broadband customers and set fees for services

Net Neutrality or De-regulation? (cont.)

- Should companies be permitted to exclude or give special treatment to content transmitted based on the content itself or on the company that provides it?
- Should companies be permitted to provide different levels of speed at different prices?

- Net Neutrality
  - Argue for equal treatment of all customers
- De-regulation
  - Flexibility and market incentives will benefit customers

Net Neutrality

Pros

- Equal treatment of all customers, content
- Not enough competition among network providers to ensure fairness
- Consistent with other common carrier practices

Cons

- Flexibility and market incentives will benefit customers
- Companies should be permitted to provide different levels of speed at different prices
- Companies should be permitted to exclude or give special treatment to certain content

FCC Net Neutrality Order (2010)

- **Transparency. Fixed and mobile broadband providers must disclose the network** management practices, performance characteristics, terms and conditions of their broadband services
- **No blocking. Fixed broadband providers may not block lawful content, applications,** services, or non-harmful devices; mobile broadband providers may not block lawful websites, or block applications that compete with their voice or video phone services
- No unreasonable discrimination. **Fixed broadband providers may not unreasonably** discriminate in transmitting lawful network traffic
- Court challenges still on-going

Legal Protection to IP

- Copyright – written or artistic expressions fixed in a tangible medium. Books, poems, songs, movies, works of art. Protects the manifestation.
- Patents – invention of any new, useful, and non-obvious process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof. Protects the idea.

Legal Protection to IP

- Trade marks – name, word, logo, symbol, etc. used to identify a product and/or service. Protects both manifestation and idea.

Patent

- You register with the government. Can register in foreign countries. US patent is issued by USPTO
  - Registration may take more than a year
- You gain the right to exclude others from making, using, or offering for sale the invention
- Patents generally last for 20 years
- Once you hold a patent, others can apply to license your invention
- Types - Utility, design, chemical, software, etc.

Copyright Holders' Exclusive Rights

- A copyright is valid for the lifetime of the author plus 70 years
- making copies
- distributing copies
- producing derivative works, such as translations into other languages or movies based on books
- performing the work in public (e.g. music, plays)
- displaying the work in public (e.g. artwork, movies, computer games, video on a Web site)

Copyright History

- 1790 first copyright law passed in US (1710 in UK)
- Copyright Act of 1909 defined an unauthorized copy as a form that could be seen and read visually
- 1976 and 1980 copyright law revised to include software and databases that exhibit "authorship" (original expression of ideas), included the "Fair Use Doctrine“
  - 1976 law stated that the copy is in violation if the original can be perceived, reproduced, or otherwise communicated by or from the copy, directly or indirectly – an improvement over “seen and read visually”

Copyright History (cont.)

- 1982 high-volume copying of records and movies became a felony
- 1992 making multiple copies for commercial advantage and private gain became a felony
  - >10 copies, worth >$2,500 get up to 5 yrs in jail
- 1997 No Electronic Theft Act made it a felony to willfully infringe copyright by reproducing or distributing one or more copies of copyrighted work with a total value of more than $1,000 within a six-month period (profit provision dropped)

Copyright History (cont.)

- 1998 Digital Millennium Copyright Act (DMCA)
  - Anti-circumvention provisions: prohibits making, distributing or using tools to circumvent technological copyright protection systems
  - Safe-harbor provisions: Protects Web sites if they remove material when asked by the copyright holder, which offered protection from some copyright lawsuits for Web sites where users post materials
- 2005 Congress made it a felony to record a movie in a movie theater

Fair Use Doctrine (1976 Law)

- Goals of copyright law is to promote production of useful work and encourage the use and flow of information
- Examples of fair use:
  - Quoting a portion in a review
  - Education (even making multiple copies for classroom use)

Fair Use Doctrine (1976 Law)

- Four factors to determine fair use
  1. Purpose and nature of use – e.g., commercial
  2. Nature of the copyrighted work (novel less likely than factual)
  3. Amount and significance of the portion used
  4. Effect of use on potential market or value of the copyrighted work (will it reduce sales of work?)
- No single factor alone determines, not all factors given equal weight, depends on circumstances

Significant Cases (1)

Sony v. Universal City Studios (1984)

- Sony made Betamax video cassette recording (VCR) machines, which were used to record movies shown on TV
- Supreme Court decided that the makers of a device with legitimate uses should not be penalized because some people may use it to infringe on copyright
- Supreme Court ruled that recording a movie for later viewing was fair use

Significant Cases (2)

Reverse engineering: game machines

- Reverse engineering: translate a program from machine code to a form that can be read and understood
  - Sega Enterprises Ltd. v. Accolade Inc. (1992)
  - Atari Games v. Nintendo (1992)
  - Sony Computer Entertainment, Inc. v. Connectix Corporation (2000)

Significant Cases (2)

- Courts ruled that reverse engineering (to learn how one platform works so that a company can make a compatible product) does not violate copyright if the intention is to make new creative works (video games), not copy the original work (the game systems)

Significant Cases (3): Napster

Sharing music: the Napster case (2001)

- Napster provided a way for users to exchange music files (no files retained on Napster site)
- Metallica filed suit against Napster – followed by A&M
- Was the sharing of music via Napster fair use?

Significant Cases (3): Napster

- Napster's arguments for fair use
  - The Sony decision allowed for entertainment use to be considered fair use
  - People make copies for personal, not commercial, use
  - Did not hurt industry sales because users sampled music on Napster and bought the CD they liked

Napster (cont’d)

- RIAA (Recording Industry Association of America)'s arguments against fair use
  - "Personal" meant very limited use, not trading with thousands of strangers
  - Songs and music are creative works and users were copying whole songs
  - Claimed Napster severely hurt sales
- Court ruled sharing music via large-scale copying on Napster violated copyright

Significant Cases (4)

File sharing: MGM v. Grokster (2005)

- Grokster, Gnutella, Morpheus, Kazaa, and others provided peer-to-peer (P2P) file sharing services
  - The companies did not provide a central service or lists of songs, but the software for sharing files
  - P2P file transfer programs have legitimate uses
- Lower Courts ruled that P2P does have legitimate uses
- Supreme Court ruled that intellectual property owners could sue the companies for encouraging copyright infringement

The Digital Millennium Copyright Act 1998

- Anti-circumvention
  - Prohibit circumventing technological access controls and copy-prevention systems
- Safe harbor
  - Protect Web sites from lawsuits for copyright infringement by users of site

The DMCA vs. Fair Use, Freedom of Speech, and Innovation

- Lawsuits have been filed to ban new technologies
- U.S. courts have banned technologies such as DeCSS even though it has legitimate uses, while courts in other countries have not
  - CSS: content scrambling system, to protect movies
- Protesters published the code as part of creative works (in haiku, songs, short movies, a computer game and art)
- U.S. courts eventually allowed publishing of DeCSS, but prohibited manufacturers of DVD players from including it in their products

Safe Harbor

- Industry issues "take down" notices per the DMCA
- As long as sites like YouTube and Facebook comply with take down notices they are not in violation
- Take down notices may violate fair use, some have been issued against small portions of video being used for educational purposes
- In addition, entertainment companies argue YouTube should have the responsibility to filter out copyright-infringement material
  - YouTube said it cannot always tell which are unauthorized

Free Software

- Free software is an idea, an ethic, advocated and supported by large, loose-knit group of computer programmers who allow people to copy, use, and modify their software
- Free means freedom of use, not necessarily lack of cost
- Open source - software distributed or made public in source code (readable and modifiable)
- Proprietary software - commercial, sold in object code, obscure, not modifiable. E.g., Microsoft Office

GNU project

- Began with a UNIX-like operating system, a sophisticated text editor, and many compilers and utilities
- Now has hundreds of programs freely available and thousands of software packages available as free software (with modifiable source code)
- Developed the concept of *copyleft*