Three case studies

- **peer to peer networking**
- **wireless systems**
- **search engines**

- **each includes issues of**
  - hardware
    processors, storage, peripherals, networks, ...
    representation of information, analog vs. digital, bits & bytes
  - software
    applications, operating system, client-server and peer to peer
    organization of information, file systems, ...
    algorithms: searching, sorting, compression
  - communications,
    Internet, Web, TCP/IP, protocols
    bandwidth, speed, caching
    compression, error detection and correction
  - security and privacy; cryptography
  - intellectual property
  - social & legal & policy concerns

Peer to peer networking

- **direct connections between peers**
  - distributed instead of clients talking to single server
  - all clients provide bandwidth, storage, processing
- **an old idea, though with a new name**
  - USENET news service, 1979 (still in use)

- **"peer-to-peer" file-sharing**
  - centralized directories (original Napster)
  - decentralized directories (Gnutella, Kazaa, Limewire, Morpheus, etc.)
- **once a file is found somewhere**
  - direct connection between supplier and consumer ("peers")
  - applications use TCP/IP (same level as HTTP, SSH, SMTP, etc.)

- **other examples**
  - BitTorrent file distribution system
  - Skype Internet telephony

Peer to peer highlights

- **Napster (1999-2001) [Shawn Fanning]**
  - centralized real-time directory, distributed files
  - mostly MP3 music; ideal for Ethernet bandwidths
  - based in USA; lawsuits put it out of business
- **Gnutella and friends (Grokster, Kazaa, ...)**
  - decentralized directories: not as fast or reliable but less vulnerable to legal processes since no way to turn it off
- **BitTorrent (2001)**
  - distributed directories, distributed files
  - distributed peer servers for load-sharing: good for movies
- **Digital Rights Management (DRM) systems**
  - largely unsuccessful (awkward, inconvenient, don't really work anyway)
  - pay services like iTunes with reasonable DRM do better
- **legal action**
  - RIAA/MPAA lawsuit put Grokster out of business (2005)
  - numerous lawsuit threats against students and other individuals
  - Viacom sues Google over YouTube postings of movies & TV programs (2007)
- **lobbying**
  - numerous attempts to create more laws against file-sharing

BitTorrent

- **file-sharing for big files in high demand**
- **original file exists on at least one "seed" site**
- **"tracker" server knows who has what pieces**
  - coordinates all transfers but does not have any of the file contents
- **clients download blocks of file from multiple sources in parallel**
  - blocks have cryptographic checksum to verify correct content
- **downloaded blocks also then uploaded to others**
  - download rate limited by upload rate: have to contribute
  - tracker knows download and upload statuses
    balances traffic, favors sites that are cooperating
- **blocks reassembled by client**
  - when client has the whole file, it can be a seed for further transfers
- **much faster than single server for right kind of use**
  - less vulnerable to flash crowds
  - but takes time to get started, can't do streaming, etc.

Internet telephony

- **Voice over IP**
  - package speech in IP packets
  - may connect to public telephone network on each end
  - strict requirements on delay (latency), jitter (variable delay), error handling, etc.
- **lots of commercial providers (AT&T, Cablevision, Verizon, Vonage,...)**
  - alternative to conventional telephone service
  - somewhat cheaper, probably less reliable, maybe fewer services
- **Skype: peer to peer VoIP**
  - comes from creators of Kazaa (!), claims no spyware or adware
  - free within Internet, ~2 cents/min to connect to regular phone system
  - 256-bit AES to encrypt each call, RSA to establish AES session key
  - proprietary protocol, uses both TCP and UDP
  - it can use your computer as a supernode (like Kazaa)
  - Skype bought by eBay 10/05 for $2.5B, sold again 11/09 for $2B

Technology meets law/policy/economics/politics

- **should there be laws controlling peer to peer technology?**
- **should content providers like RIAA be permitted to install search (& destroy) software on home computers?**
- **should universities be required to enforce file-sharing laws?**
- **should VoIP be regulated by the FCC?**
  - should VoIP suppliers have to provide services like 911?
  - should VoIP suppliers pay taxes and fees, and for connectivity to public telephone network?
  - should VoIP calls be subject to wire-tapping laws like regular phones?
- **should common carriers like Verizon be permitted to discriminate against traffic from other VoIP suppliers?**
  - should there be different prices and policies for different kinds of traffic?

Net neutrality

- **Comcast interfering with some BitTorrent traffic**
  - claimed to be legitimate network management action to prevent a service from hogging bandwidth
  - when does a common carrier have the right to discriminate against some kinds of traffic to provide service to other kinds?
  - FCC told Comcast to stop; Comcast appealed in court (in process)
- **Verizon redirecting failed DNS queries to its own search page**
  - instead of simply returning the failure status
  - clear violation of a standard protocol
  - breaks unrelated services (e.g., non-browser traffic)
  - overrides consumer choice of services
- **what regulations, if any, should there be?**
- **Ed Felten paper: http://itpolicy.princeton.edu/pub/neutrality.pdf**

Copyright issues

- **digital media are intrinsically easy to copy**
  - and hard to protect by technical means
- **peer to peer enables copyright violation on a grand scale**
- **Digital Millennium Copyright Act (DMCA)**
- **test cases**
- **disclaimer**
  - an enormous topic
  - IANAL

Copyright

- **protects expression, not idea**
- **duration used to be 17 years + one renewal**
- **now life + 70, or 95 for commercial works**
  - (the "Mickey Mouse Protection Act", 1998)
- **"fair use" permits limited copying under some circumstances**
  - criticism, comment, scholarship, research, news reporting, teaching
- **uncertain what fair use really is -- case by case decisions**
- **considerations:**
  - purpose and character of the use
  - nature of the copyrighted work
  - amount and substantiality of the portion used
  - effect of the use on potential market or value of copyrighted work
- **recent copyright laws may prevent some fair uses**
  - can't decrypt to make excerpt for teaching or criticism
  - can't reverse engineer to make copies in different media

DMCA: Digital Millennium Copyright Act (1998)

- **US copyright law: www.copyright.gov/title17, Chapter 12**

- **anticircumvention: illegal to circumvent a technological measure protecting access to or copying of a copyrighted work**
  - limited exceptions for reverse engineering for interoperability, encryption research, security testing

- **illegal to remove or alter copyright notices and management information**

- **"safe harbor": protects ISPs from copyright infringement claims if they follow notice and takedown procedures**

Reporting copyright infringement

To report copyright infringements involving Princeton University information technology resources or services, please notify:

Rita Seplowitz Saltz
Princeton University
87 Prospect Avenue
Princeton, NJ 08544

E-mail: rita@Princeton.EDU
Phone: (609) 258-6066
Fax: (609) 258-3943

Ms. Saltz, Princeton University Office of Information Technology, is acting in conjunction with Princeton Universit Office of the General Counsel as the agent designated unde the Digital Millennium Copyright Act, P.L. 105-304, to respond to reports alleging copyright infringements on Princeton University Web site locations.

Members of the University community who engage in any activity that infringes copyright-protected materials may be subject to disciplinary action. Under circumstances involving repeated instances of infringement through the use of the University's computing network, such disciplinary action may include the termination or suspension of network privileges.

Information that must be provided in complaints

The Digital Millennium Copyright Act specifies that all infringement claims must be in writing (either electronic mail or paper letter) and must include the following elements:

1. a physical or electronic signature;
2. identification of the infringed work;
3. identification of the infringed material;
4. contact information for the complainant, e.g. address, telephone number, electronic mail address;
5. a statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner or the law; and
6. a statement that the information contained in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the copyright owner.

DMCA test cases

- **Grokster**
  - peer to peer software makes copyright infringement easy; are its distributors violating the DMCA?
- **Diebold**
  - internal emails reveal flaws in voting machine software; is posting of the emails a violation of DMCA?
- **SDMI**
  - does demonstration of how to remove digital watermarking on audio files violate DMCA?
- **Lexmark**
  - cryptography used to prevent 3rd parties from supplying replacement ink cartridges; is reverse engineering a violation of DMCA?
- **DeCSS**
  - does publication of code to defeat content scrambling system used to protect DVDs from copying violate DMCA?
- ...

DRM

- **techniques to control access to and use of digital material**
  - largely unsuccessful
- **CSS (content scramble system) encrypts DVDs to prevent playing except on licensed players (and thus prevent copying)**
  - cracked by "DVD Jon"
- **AACS (advanced access control system) encrypts HD-DVD and Blu-Ray**
  - cracked in 2007
- **Windows Media DRM**
  - cracked in 2006-7
- **iTunes FairPlay**
  - cracked in 2006
- **Sony rootkit on audio CDs (2005)**
  - discovered immediately
- **etc.**

Digital (Rights or Restrictions?) Management

- **a disguised form of vendor lock-in?**
- **conflicts with fair use**
  - prevents legitimate operations like time/space shifting, media conversion, backup, ...
- **obsolescent technology may cause things to be lost**
- **incompatible systems make users unhappy**
  - may cause more trouble that it's worth
- **pragmatically, DRM doesn't work and probably can't**
  - long history of failed / cracked systems
  - the analog hole as the last resort