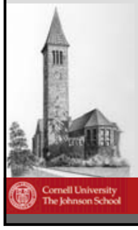


NBA 600
DRM and Darknets
Class 7, Tue 11/6
(Originally Monday 11/5)

Prof. Dan Huttenlocher

Administrative

- In-class final presentations, Wed 11/28
  - – Okonmah, Farhangi, Figlioni – Digital Music
  - – Golden, Slowik, Wilks – Virtual Worlds Retail
  - – Lim, Moth, Johnson – Patient Health Records
  - – Fritz, Adelco, Chang – Digital Banking
- Others hand in final paper, 12/7 by noon

Today’s Class

- Digital rights management (DRM)
  - – Technical means for controlling digital content
  - – DMCA – Digital Millennium Copyright Act
- Darknets
  - – Unauthorized networked sharing of digital content

Recap DMCA

- Digital Millennium Copyright Act
  - – Passed in October 1998 in response to Internet
  - – Also part of WIPO copyright treaty
- Ban on creating technological tools that can be used to violate copyright
  - – Rather than just on copyright violation itself
  - – Implications for fair use
    - • No person shall circumvent a technological measure that effectively controls access
      - – Copying that may otherwise be allowed can be prevented with copy protected digital goods

Justification For DMCA

- Traditional copyright strongly tied to physical copying – different in Internet age
  - – Some electronic copies a necessary part of experiencing digital content
  - – Other electronic copies a large threat to owners’ rights
  - – Owner can best govern with new technologies
    - • As long as others interdicted from circumvention
- Note parallels to biotechnology
  - – Plants with seeds that don’t germinate, a technological solution to unauthorized re-use

Breadth of DMCA

- Digital Rights Management (DRM) technology has broad range of uses beyond limiting copying
  - – How authorized user can experience content
    - • On what devices, at what times, number of copies, etc.
  - – Can enable pricing mechanisms other than “buying a copy”
    - • Per use, rental, etc.
  - – Protection of any device with digital content
    - • Tried for many things, e.g. toner cartridges

DRM Technologies

- Provide content (generally encrypted) with specification of how it can be used
  - DRM system must be “trusted” to limit usage
  - Only give key to decrypt content to such trusted parties
  - Weakness of DRM schemes
    - BOBE (break once break everywhere) resistance
- Wide variety of use restrictions
  - CSS for DVDs allows “viewing” not “copying”
  - Restrictions on numbers of copies, devices, …

DVD Copy Protection

- Each trusted device has a secret key that is used to identify it
  - Such devices don’t allow decrypted (usable) content to be copied
    - E.g., consumer DVD players okay but not computer DVD drives
    - Microsoft media player okay but not software in general
- Each DVD stores encrypted device keys of trusted devices
  - Playing DVD requires match to device key

Flawed DVD Protection

- A fundamental problem with CSS made it relatively easy to duplicate keys
  - Keys were supposed to be stored encrypted so they could not be copied
    - A manufacturer accidentally released an un-encrypted key
  - A flaw in the scheme made it quite easy to create many keys given a single key
    - deCSS - keys and software for de-scrambling DVDs rapidly distributed on the Internet
- “DVD Jon” tried in Norway, acquitted

DMCA and E-Book Reader

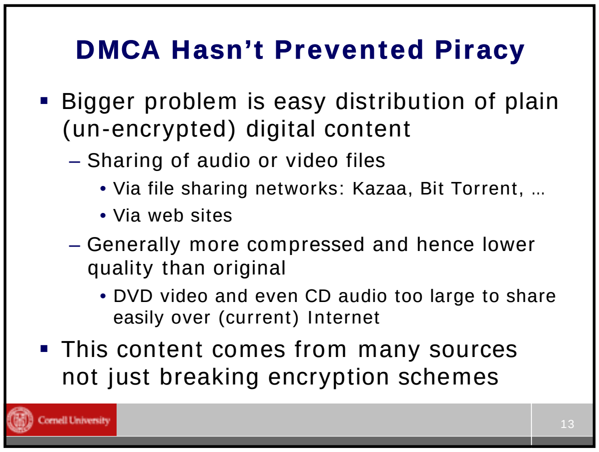
- Russian company Elcomsoft and programmer sued by US Attorney in S.F.
  - First criminal application of the law
- For reverse engineering Adobe’s E-Book reader software
  - Permitting users to decrypt electronic books
  - Adobe dropped its support of case against programmer after protests by its own staff
- Jury acquitted company in Dec. 2002
  - Based on company’s speedy removal of offending software on Adobe’s request

Apple’s Fairplay

- Apple’s DRM called Fairplay
  - Limits where iTunes content can be played
  - Also what protected content will play on iPods
- DVD Jon’s company DoubleTwist has announced it has reverse engineered Fairplay DRM, offering two products
  - Allow other protected content to be played on iPods
  - Allow iTunes content to be played on other devices
    - Legality unclear, “interoperability”

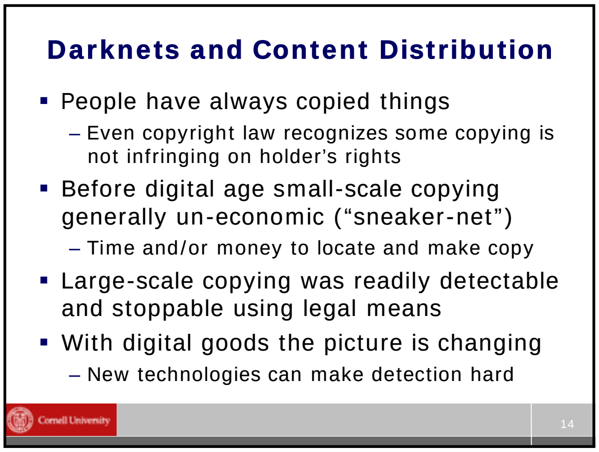
DRM and New Markets

- Creation of derivative works
  - Used to just be professionals
  - Now use of music, samples, clips in personal videos and other forms of expression
- Myspace
  - Not just unsigned bands or complete copyrighted works
- YouTube
  - Problems even determining what infringes and who to license from



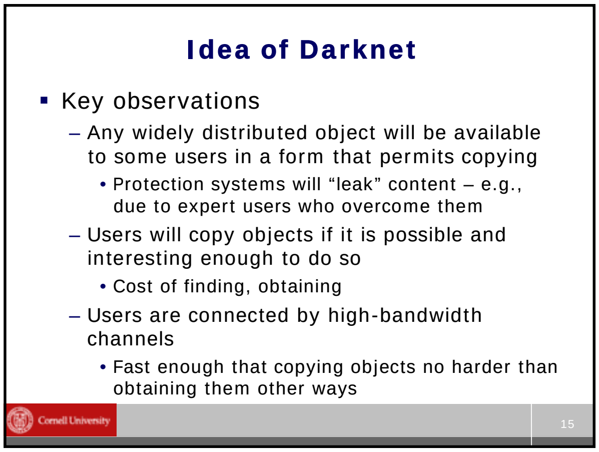
DMCA Hasn't Prevented Piracy

- Bigger problem is easy distribution of plain (un-encrypted) digital content
  - Sharing of audio or video files
    - Via file sharing networks: Kazaa, Bit Torrent, …
    - Via web sites
  - Generally more compressed and hence lower quality than original
    - DVD video and even CD audio too large to share easily over (current) Internet
- This content comes from many sources not just breaking encryption schemes



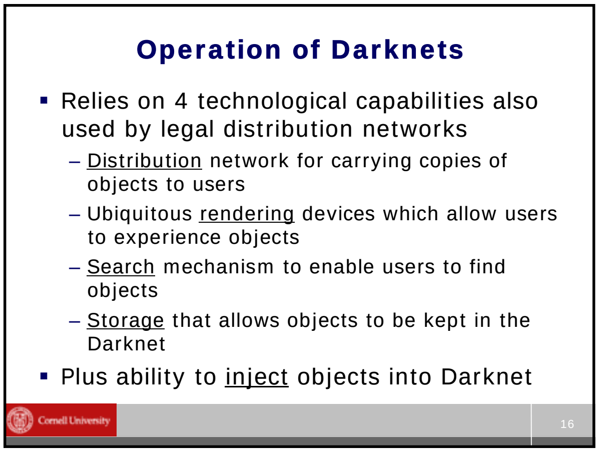
Darknets and Content Distribution

- People have always copied things
  - Even copyright law recognizes some copying is not infringing on holder's rights
- Before digital age small-scale copying generally un-economic ("sneaker-net")
  - Time and/or money to locate and make copy
- Large-scale copying was readily detectable and stoppable using legal means
- With digital goods the picture is changing
  - New technologies can make detection hard



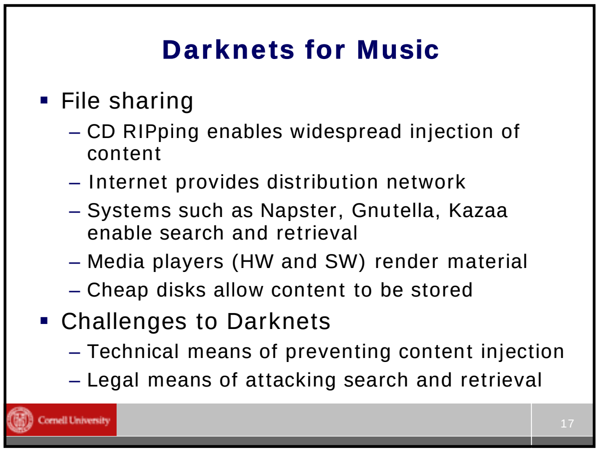
Idea of Darknet

- Key observations
  - Any widely distributed object will be available to some users in a form that permits copying
    - Protection systems will "leak" content – e.g., due to expert users who overcome them
  - Users will copy objects if it is possible and interesting enough to do so
    - Cost of finding, obtaining
  - Users are connected by high-bandwidth channels
    - Fast enough that copying objects no harder than obtaining them other ways



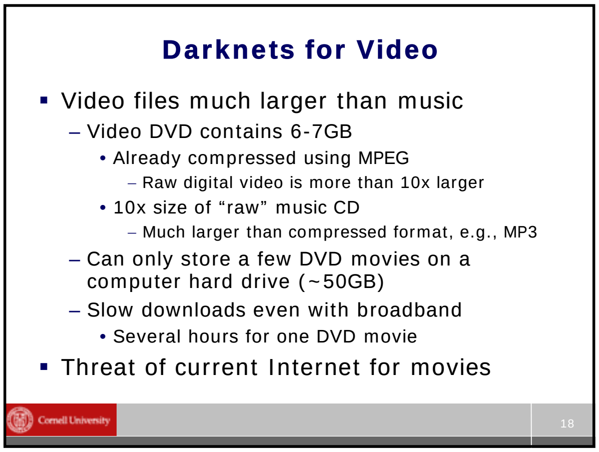
Operation of Darknets

- Relies on 4 technological capabilities also used by legal distribution networks
  - Distribution network for carrying copies of objects to users
  - Ubiquitous rendering devices which allow users to experience objects
  - Search mechanism to enable users to find objects
  - Storage that allows objects to be kept in the Darknet
- Plus ability to inject objects into Darknet



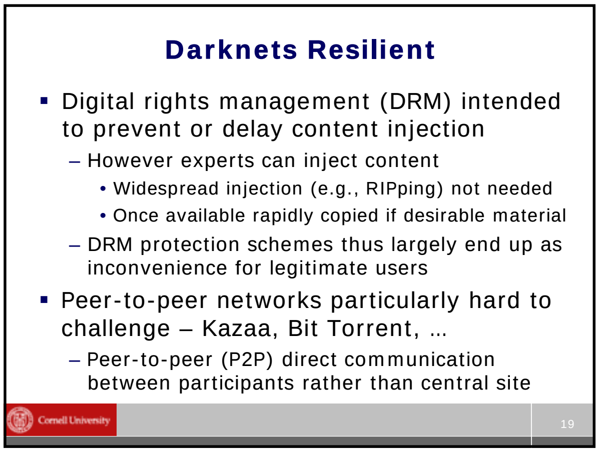
Darknets for Music

- File sharing
  - CD RIPping enables widespread injection of content
  - Internet provides distribution network
  - Systems such as Napster, Gnutella, Kazaa enable search and retrieval
  - Media players (HW and SW) render material
  - Cheap disks allow content to be stored
- Challenges to Darknets
  - Technical means of preventing content injection
  - Legal means of attacking search and retrieval



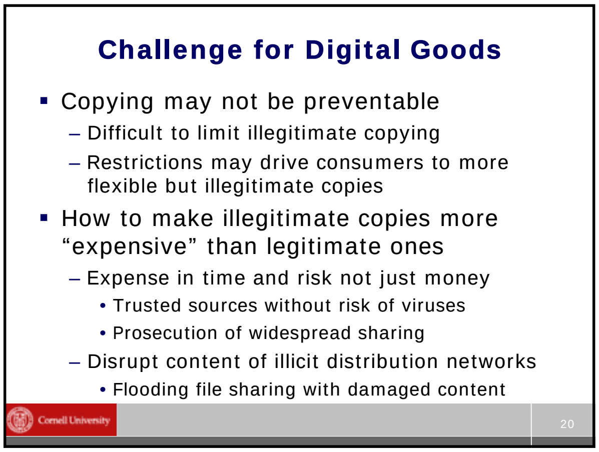
Darknets for Video

- Video files much larger than music
  - Video DVD contains 6-7GB
    - Already compressed using MPEG
      - Raw digital video is more than 10x larger
    - 10x size of "raw" music CD
      - Much larger than compressed format, e.g., MP3
  - Can only store a few DVD movies on a computer hard drive (~50GB)
  - Slow downloads even with broadband
    - Several hours for one DVD movie
- Threat of current Internet for movies



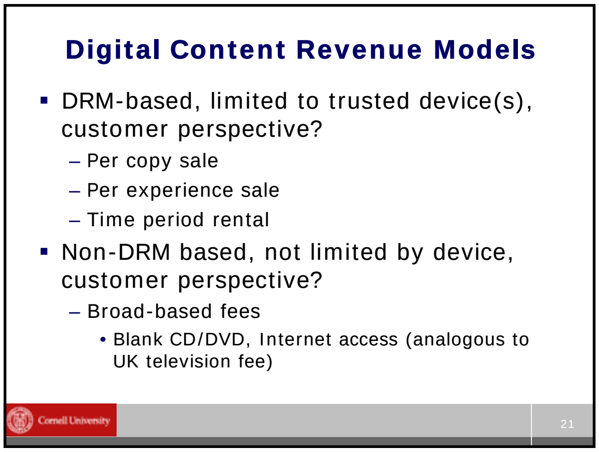
Darknets Resilient

- Digital rights management (DRM) intended to prevent or delay content injection
  - – However experts can inject content
    - • Widespread injection (e.g., RIPping) not needed
    - • Once available rapidly copied if desirable material
  - – DRM protection schemes thus largely end up as inconvenience for legitimate users
- Peer-to-peer networks particularly hard to challenge – Kazaa, Bit Torrent, …
  - – Peer-to-peer (P2P) direct communication between participants rather than central site



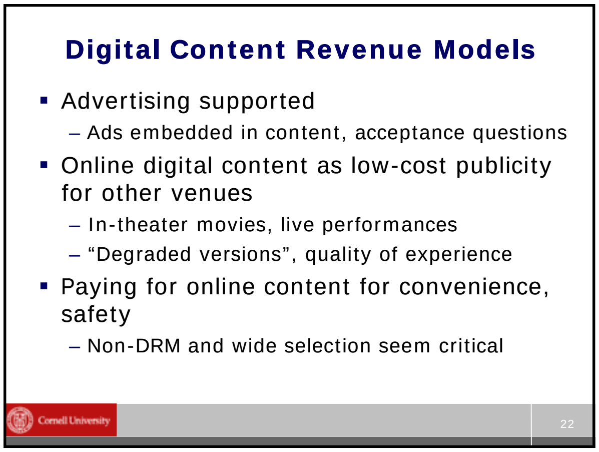
Challenge for Digital Goods

- Copying may not be preventable
  - – Difficult to limit illegitimate copying
  - – Restrictions may drive consumers to more flexible but illegitimate copies
- How to make illegitimate copies more “expensive” than legitimate ones
  - – Expense in time and risk not just money
    - • Trusted sources without risk of viruses
    - • Prosecution of widespread sharing
  - – Disrupt content of illicit distribution networks
    - • Flooding file sharing with damaged content



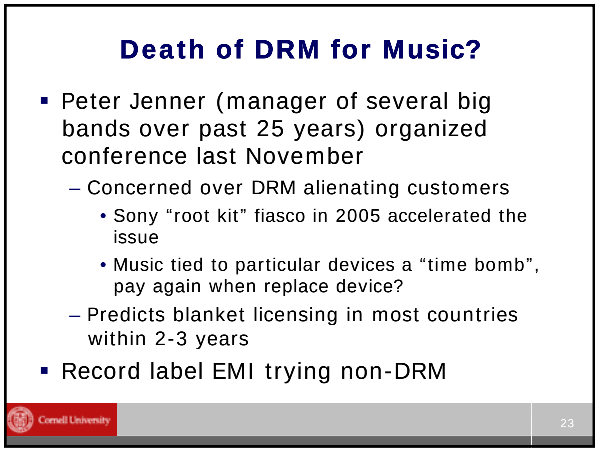
Digital Content Revenue Models

- DRM-based, limited to trusted device(s), customer perspective?
  - – Per copy sale
  - – Per experience sale
  - – Time period rental
- Non-DRM based, not limited by device, customer perspective?
  - – Broad-based fees
    - • Blank CD/DVD, Internet access (analogous to UK television fee)



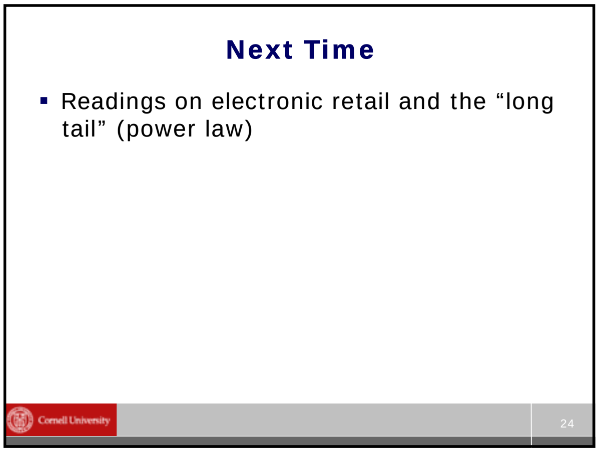
Digital Content Revenue Models

- Advertising supported
  - – Ads embedded in content, acceptance questions
- Online digital content as low-cost publicity for other venues
  - – In-theater movies, live performances
  - – “Degraded versions”, quality of experience
- Paying for online content for convenience, safety
  - – Non-DRM and wide selection seem critical



Death of DRM for Music?

- Peter Jenner (manager of several big bands over past 25 years) organized conference last November
  - – Concerned over DRM alienating customers
    - • Sony “root kit” fiasco in 2005 accelerated the issue
    - • Music tied to particular devices a “time bomb”, pay again when replace device?
  - – Predicts blanket licensing in most countries within 2-3 years
- Record label EMI trying non-DRM



Next Time

- Readings on electronic retail and the “long tail” (power law)