WHY PIRATES (STILL) WON'T BEHAVE: REGULATING P2P TEN YEARS AFTER NAPSTER

Annemarie Bridy

Associate Professor

University of Idaho College of Law

Points of Intervention in the Culture of P2P

- Content Level Regulation
  - Digital Rights Management (DRM)
  - The Digital Millennium Copyright Act (DMCA)
- Network Level Regulation
  - "Gatekeeper" Lawsuits (Napster, Aimster, Grokster, LimeWire)
  - Traffic Surveillance by "Undercover Users"
  - Traffic Management by ISPs
    - Deep Packet Inspection (DPI)
    - Torrent Blocking or Throttling

Content Level Regulation

- Code can fix what code has broken
  - "I'm trying to put in place technological magic that can combat the technological magic that allows thievery." – Jack Valenti, former president of the MPAA
  - "Digital media are at least the right sort of thing to be regulated with software, because they are themselves creatures of software." – James Grimmelman, *Regulation by Software*

Content Level Regulation

WHY RIGHTS OWNERS LOVE DRM

- Total control over the reproduction of digital content
- Substitution of reliable computational rules for fuzzy legal standards like fair use

WHY CONSUMERS HATE DRM

- Total control over the reproduction of digital content *by someone else*
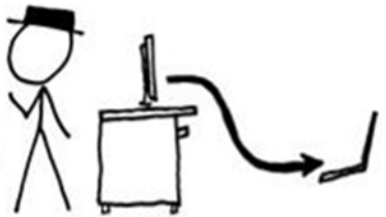- Substitution of *someone else's* reliable computational rules for fuzzy legal standards like fair use

Content Level Regulation

- The DRM Dilemma

XKCD, *Steal this Comic*

Content Level Regulation

- What the law has protected, the market has rejected
    - The DMCA prohibits distribution of software that circumvents DRM
    - DRM is "ruleish" and prevents fair uses as well as piracy
    - Frustrated consumers who can't port or restore content they've lawfully acquired turn to hackers for help
    - Circumvention tools are freely available on the Internet thanks to hackers (who are not a compliant group in the main)
    - DRM gets circumvented on a grand scale regardless of the DMCA
    - Circumvention enables piracy as well as fair use

Content Level Regulation

- Do you believe in magic? Steve Jobs doesn't:
  - "There is no theory of protecting content other than keeping secrets. In other words, even if one uses the most sophisticated cryptographic locks to protect the actual music, one must still 'hide' the keys which unlock the music on the user's computer or portable music player. No one has ever implemented a DRM system that does not depend on such secrets for its operation."

Content Level Regulation

- The DRM Dilemma: A Case in Point
  - *United States v. Elcom* (2002)
    - Advanced eBook Processor (AEBPR) – stripped DRM from eBooks
    - DRM allowed eBook copyright owners to prevent copying, printing, "lending" by one user to another on the same network, or viewing on any computer other than the original download destination
    - AEBPR allowed users to read eBooks on a second computer, make a back-up digital copy, or print the eBook in paper form
    - Court blocked distribution of AEBPR under the DMCA, because it enabled infringement as well as fair use

Content Level Regulation

- Why has DRM failed as a regulatory mechanism?
  - A technical answer
    - Code can break what code fixes
    - The "magic" of DRM relies, at base, on a conceptually primitive system of locks and keys
  - A normative answer
    - DRM prevents users from doing what they *should* be able to do in order to prevent them from doing what they *shouldn't*
    - Failure to discriminate between fair and "foul" uses leads to loss of legitimacy in eyes of consumers

Content Level Regulation

- The Problem with Locks & Keys: A Case in Point
  - Jon Johansen (DVD Jon) (1999)
    - DeCSS – unlocks the Content Scrambling System (CSS) of encryption on DVDs
    - CSS prevents DVDs from being played on unlicensed players
    - Johansen wanted to be able to play DVDs he had bought on a PC running the Linux O/S
    - He was 16 years old (!) when he cracked CSS
    - Hollywood's "technological magic" is no match for an enterprising teenager

Content Level Regulation

- How do we know that DRM has failed as a regulatory mechanism?

The New York Times

Want to Copy iTunes Music? Go Ahead, Apple Says

By BRAD STONE
Published: January 6, 2009

SAN FRANCISCO — In moves that will help shape the online future of the music business, Apple said Tuesday that it would remove anticopying restrictions on all of the songs in its popular iTunes Store and allow record companies to set a range of prices for them.

- Amazon and Wal-Mart went 100% DRM-free even before Apple did

Network Level Regulation

- Regulation by Preliminary Injunction: Fighting P2P in the Courts
  - The Strategy
    - Target "gatekeepers": stop unauthorized copying by blocking distribution of the technology that facilitates it
  - The Cases
    - *A&M Records v. Napster* (9th Cir. 2001)
    - *In re Aimster* (7th Cir. 2003)
    - *MGM v. Grokster* (U.S. 2005)
    - *Arista v. MetaMachine* (S.D.N.Y. 2006)
    - *Arista v. LimeWire* (S.D.N.Y. 2006)

Network Level Regulation

- When is a win really a loss?
  - Rights owners won preliminary injunctions against Napster, Aimster, and Grokster for contributory infringement
  - All three services folded, but P2P lives on…
  - How is that possible?
    - *Sony v. Universal* (1984) – The Betamax Case
      - "A computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."
      - Where the technology in question is "capable of substantial noninfringing uses," its distribution will not be enjoined.

Network Level Regulation

- Problems with litigating against P2P providers
  - The *Sony* Doctrine protects P2P technology because it can be used (and is being used) for lawful purposes
  - Unless P2P providers are actively inducing acts of infringement, they are not liable for the actions of their users
  - Operators of P2P systems after *Grokster* know <u>not</u> to do or say anything that looks like inducement. And as long as they remove access to infringing content in response to takedown notices, they're not liable.

Network Level Regulation

- Regulation by surveillance

Network Level Regulation

- The RIAA hires MediaSentry, which has its investigators trawl P2P networks as "undercover users"
- They collect the IP addresses of file sharers offering copyrighted content
- Incident reports containing IP addresses, filenames, and other information become the basis for subpoenas in "John Doe" lawsuits
- Through the subpoena process, anonymous file sharers are identified for prosecution

Network Level Regulation

- Under what conditions does surveillance work as a regulatory mechanism?
  - The seer must see all (reliability)
  - The seer can't be seen (invisibility)

Network Level Regulation

- Problems with surveillance
  - Unreliability: Cases of mistaken identity
    - 66-year Sarah Ward
      - Sued in 2003 for allegedly sharing 2,000+ songs (including rapper Trick Daddy's "I'm a Thug") through Kazaa
      - She owned a Mac and could not have run Kazaa
    - 83-year old Gertrude Walton
      - Sued in 2005 – after her death in 2004 – for allegedly sharing 700 songs
      - She had never owned a computer in her life
    - Computer researchers were able to "trick" industry monitors of Torrent networks into sending a slew of takedown notices to a printer and other machines sharing no content whatsoever
      - It's pretty easy to "frame" any IP address to make it look like it's sharing copyrighted files

Network Level Regulation

- Problems with surveillance
  - Visibility: The watchers become the watched
    - Monitoring agents behave online in ways that make them "highly distinguishable" from regular BitTorrent users
    - Automatic detection of monitoring agents is feasible
    - On-the-fly blacklisting techniques will be developed to block IP addresses engaged in monitoring activity

Network Level Regulation

- Problems with surveillance
  - Unreliability: Migration of users to "darknets" or F2F networks
    - Darknets are not open to all comers in the way that LimeWire, Kazaa, and other popular file sharing services are
    - Darknets are private networks that require authentication through insider contacts, so they're hard for monitors to crack
    - Traffic flowing over darknets is often encrypted, which is an added obstacle to monitoring

Network Level Regulation

- Regulation by Surveillance: Deputizing ISPs
  - ISPs are in a better position than hired undercover monitors to be the industry's "invisible eye"
  - The industry has appealed to the self-interest of ISPs: "We're in this together!"
  - The industry has lobbied the federal government to require ISPs to police P2P networks through "technology-based deterrents" like deep packet inspection (DPI)
    - 2008 amendments to the federal Higher Education Act (HEA)

Network Level Regulation

- Problems with deputizing ISPs
  - Monitoring traffic is a *big* departure from the role that ISPs have played historically in the operation of the Internet
    - Immunity for ISPs under the DMCA is predicated on their status as mere conduits for data
  - Monitoring and blocking are threats to Net Neutrality
    - Comcast torrent blocking/throttling scandal (2007)
  - Monitoring and blocking are threats to user privacy
    - DPI may violate provisions of the Wiretap Act that prohibit the interception of communications

Network Level Regulation

- Problems with deputizing ISPs
  - Encryption defeats DPI
    - As the use of DPI by ISPs becomes more common, users will likely shift to P2P programs like Freenet that enable encryption and anonymization
      - "Communications by Freenet nodes are encrypted and are 'routed-through' other nodes to make it extremely difficult to determine who is requesting the information and what its content is."