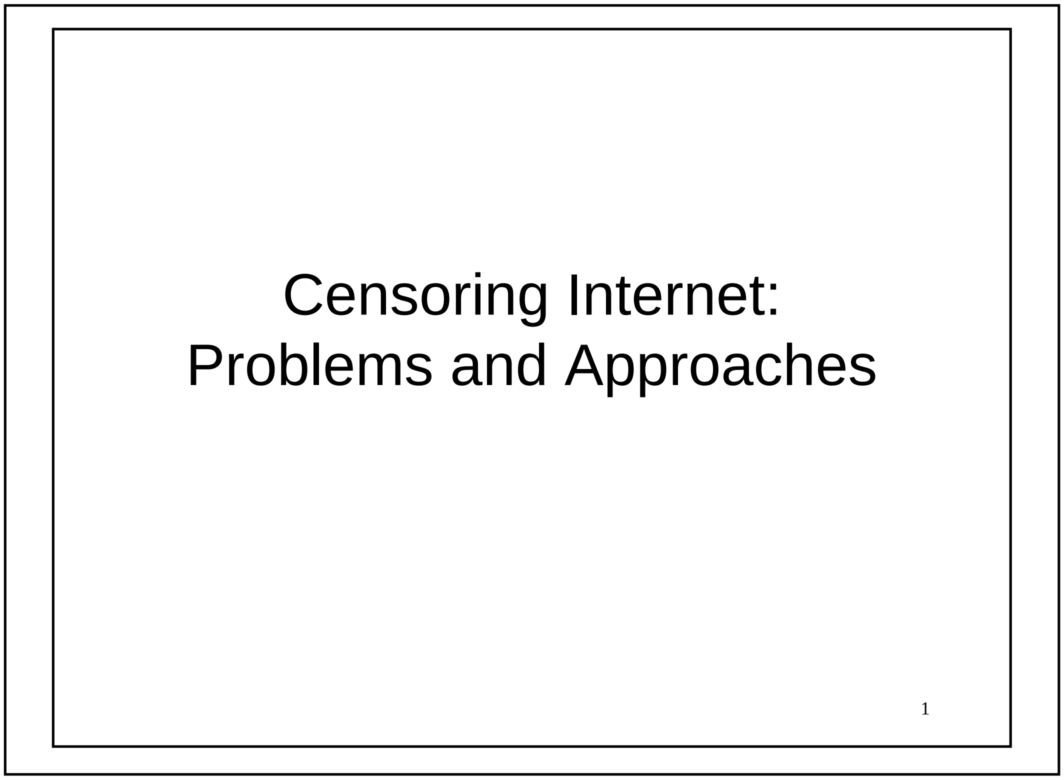
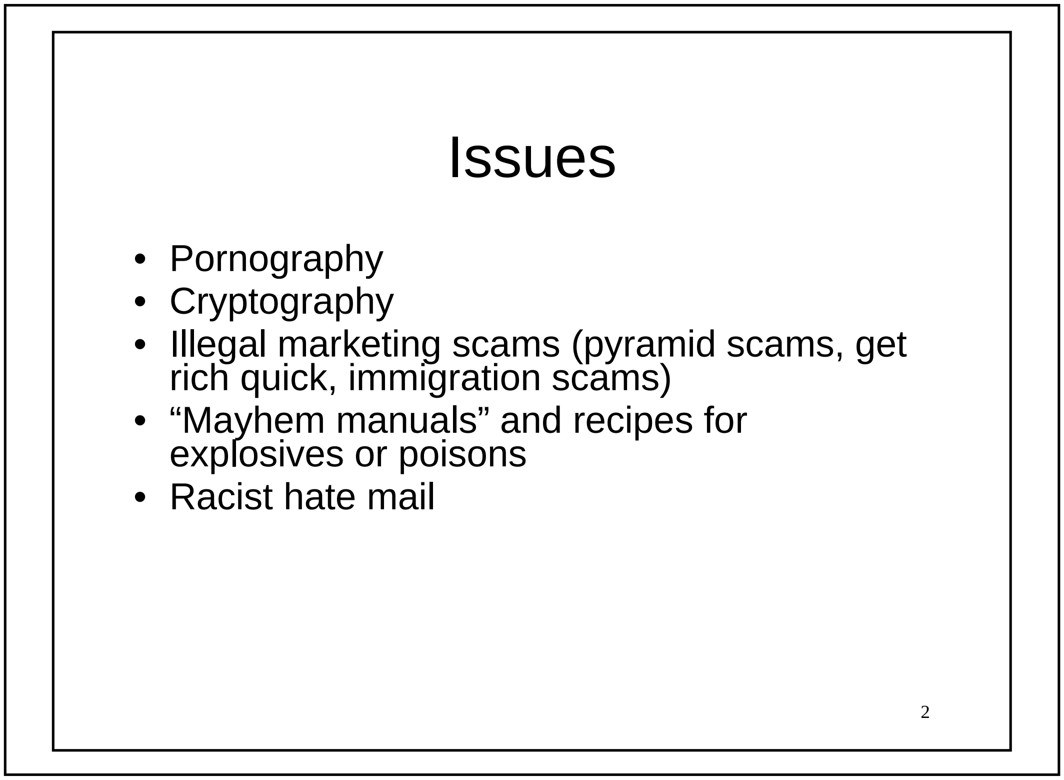


Censoring Internet: Problems and Approaches

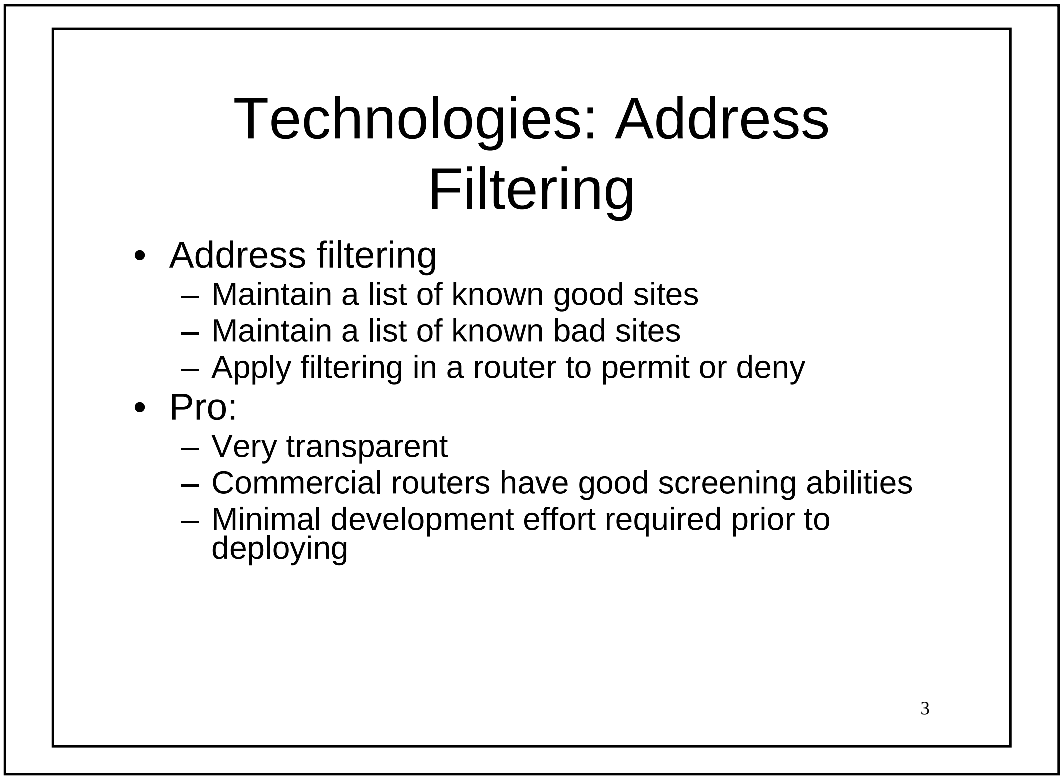
1



Issues

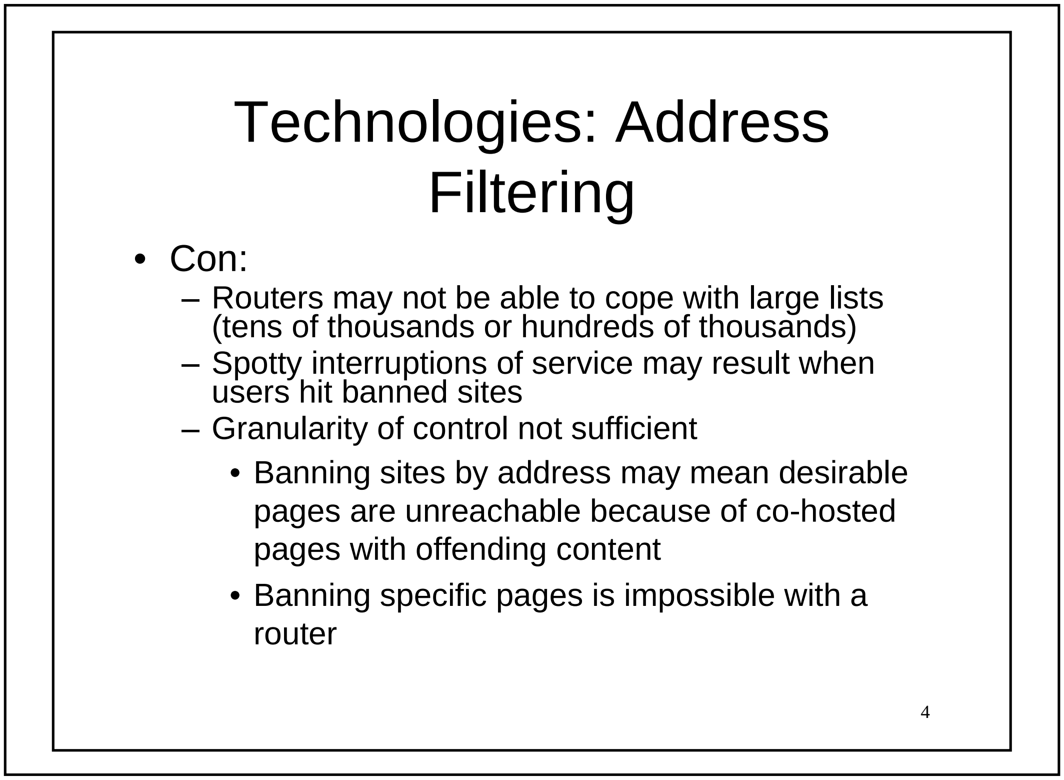
- Pornography
- Cryptography
- Illegal marketing scams (pyramid scams, get rich quick, immigration scams)
- “Mayhem manuals” and recipes for explosives or poisons
- Racist hate mail

2



Technologies: Address Filtering

- Address filtering
  - Maintain a list of known good sites
  - Maintain a list of known bad sites
  - Apply filtering in a router to permit or deny
- Pro:
  - Very transparent
  - Commercial routers have good screening abilities
  - Minimal development effort required prior to deploying



Technologies: Address Filtering

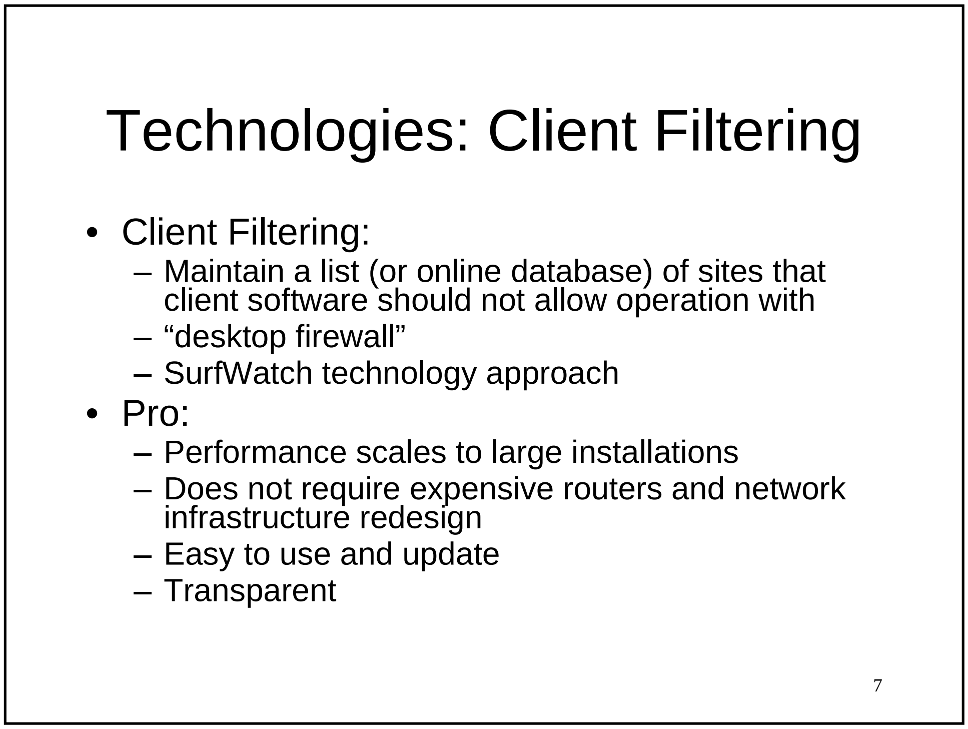
- Con:
  - Routers may not be able to cope with large lists (tens of thousands or hundreds of thousands)
  - Spotty interruptions of service may result when users hit banned sites
  - Granularity of control not sufficient
    - Banning sites by address may mean desirable pages are unreachable because of co-hosted pages with offending content
    - Banning specific pages is impossible with a router

Technologies: Firewalls

- Firewalls:
  - Use some kind of application relay technology running on a firewall host
- Pro:
  - Excellent audit trail
  - Easy to modify and scale system (buy more RAM, disk, and processor power)
  - May be a good spot to add caching for Web performance or FTP service
  - May help keep hackers out (are there hackers in Singapore?)

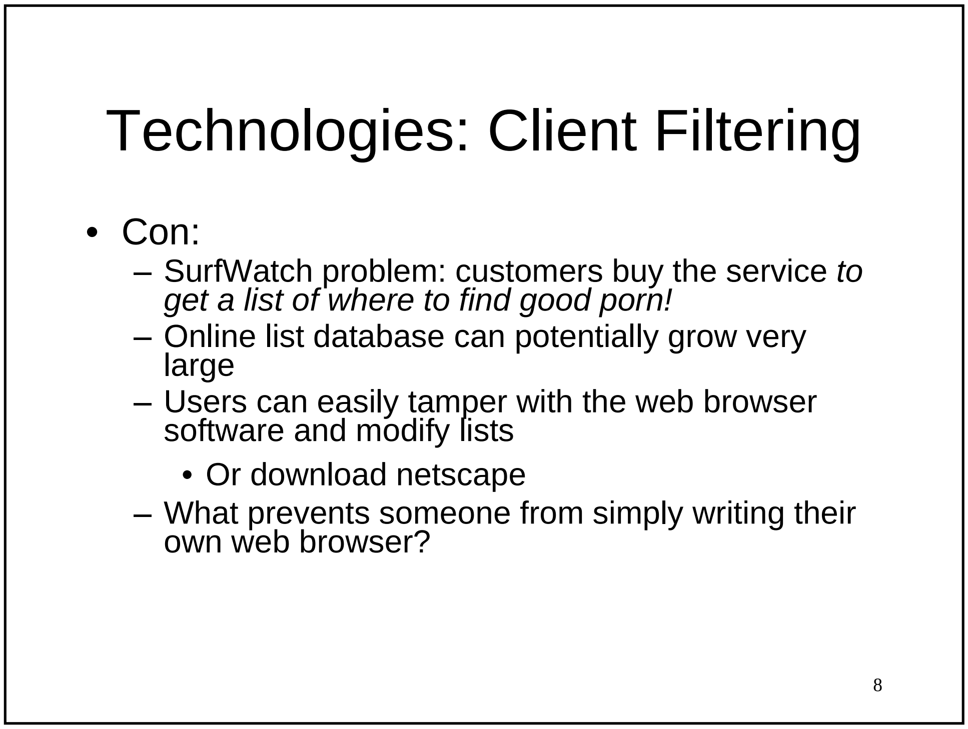
Technologies: Firewalls

- Con:
  - May be a serious performance bottleneck
  - May (depending on implementation) not be transparent
  - May not scale
    - Nobody that I know of has tried to firewall off an entire country before
    - Most UNIX machines cannot support 10,000 users
  - Slow to adapt to new technologies and services
  - Can a complete national-level security perimeter be enforced?



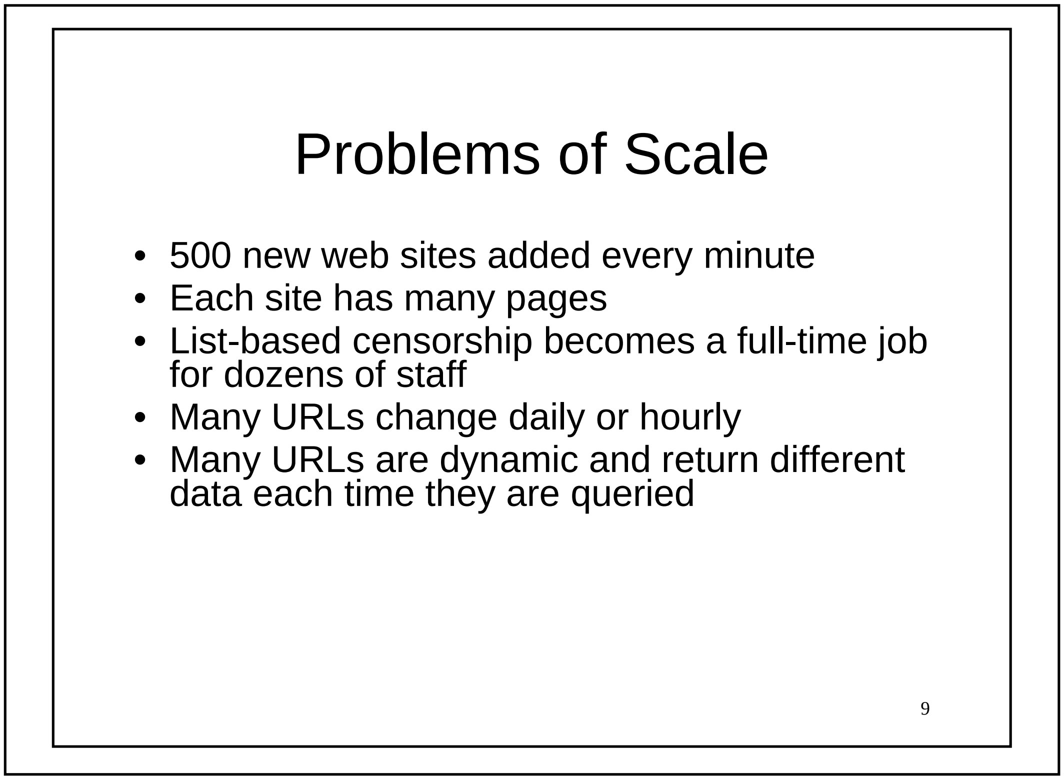
Technologies: Client Filtering

- Client Filtering:
  - – Maintain a list (or online database) of sites that client software should not allow operation with
  - – “desktop firewall”
  - – SurfWatch technology approach
- Pro:
  - – Performance scales to large installations
  - – Does not require expensive routers and network infrastructure redesign
  - – Easy to use and update
  - – Transparent



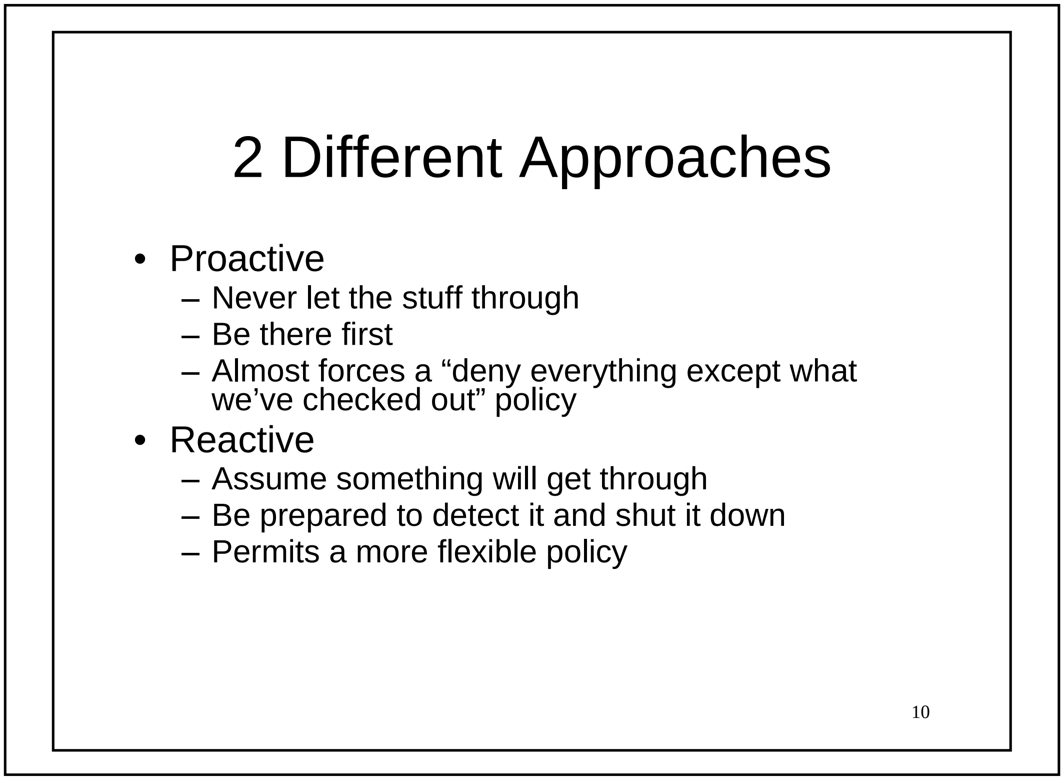
Technologies: Client Filtering

- Con:
  - – SurfWatch problem: customers buy the service *to get a list of where to find good porn!*
  - – Online list database can potentially grow very large
  - – Users can easily tamper with the web browser software and modify lists
    - Or download netscape
  - – What prevents someone from simply writing their own web browser?



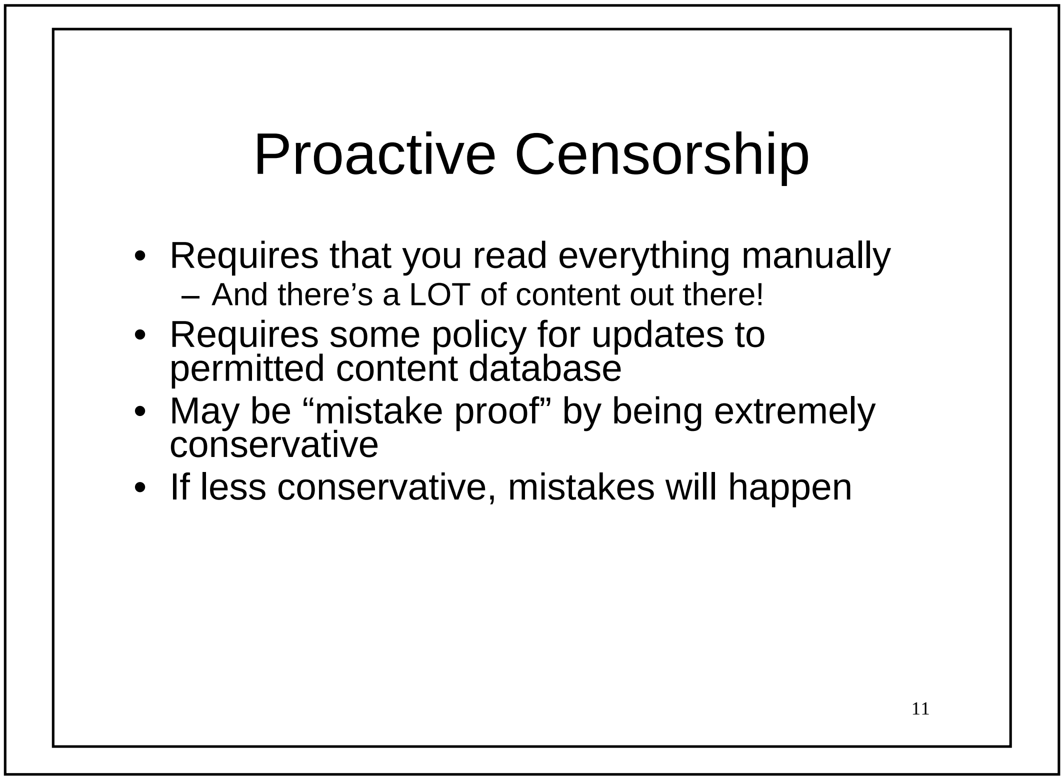
Problems of Scale

- 500 new web sites added every minute
- Each site has many pages
- List-based censorship becomes a full-time job for dozens of staff
- Many URLs change daily or hourly
- Many URLs are dynamic and return different data each time they are queried



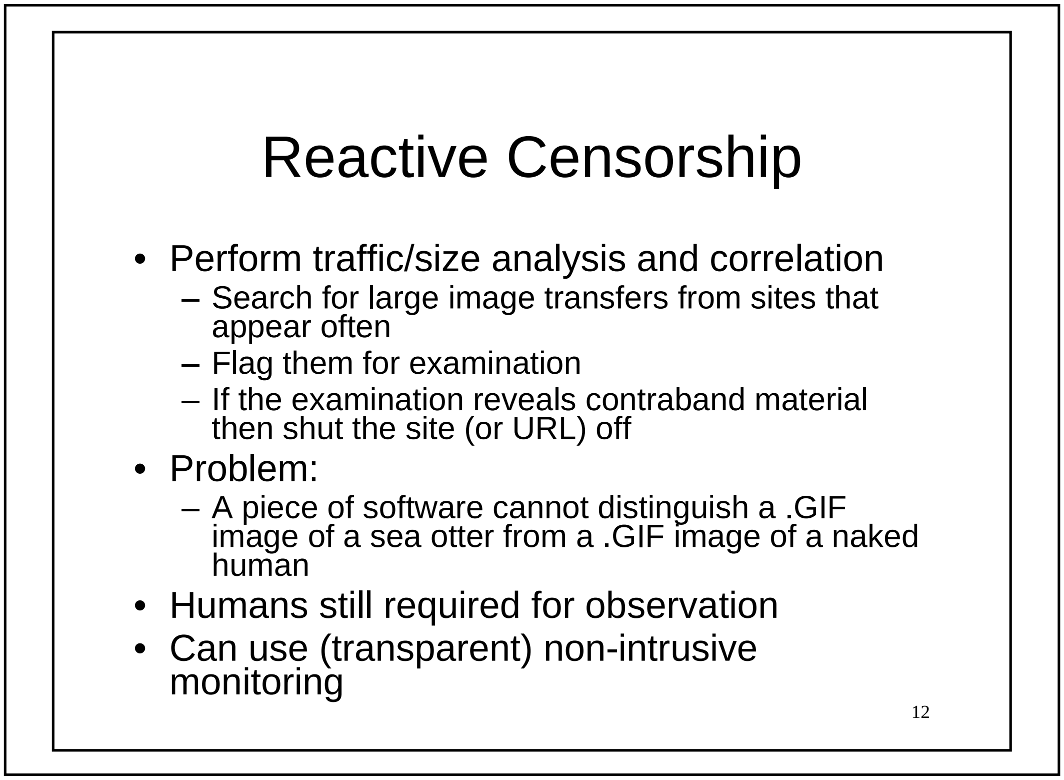
2 Different Approaches

- Proactive
  - Never let the stuff through
  - Be there first
  - Almost forces a “deny everything except what we’ve checked out” policy
- Reactive
  - Assume something will get through
  - Be prepared to detect it and shut it down
  - Permits a more flexible policy



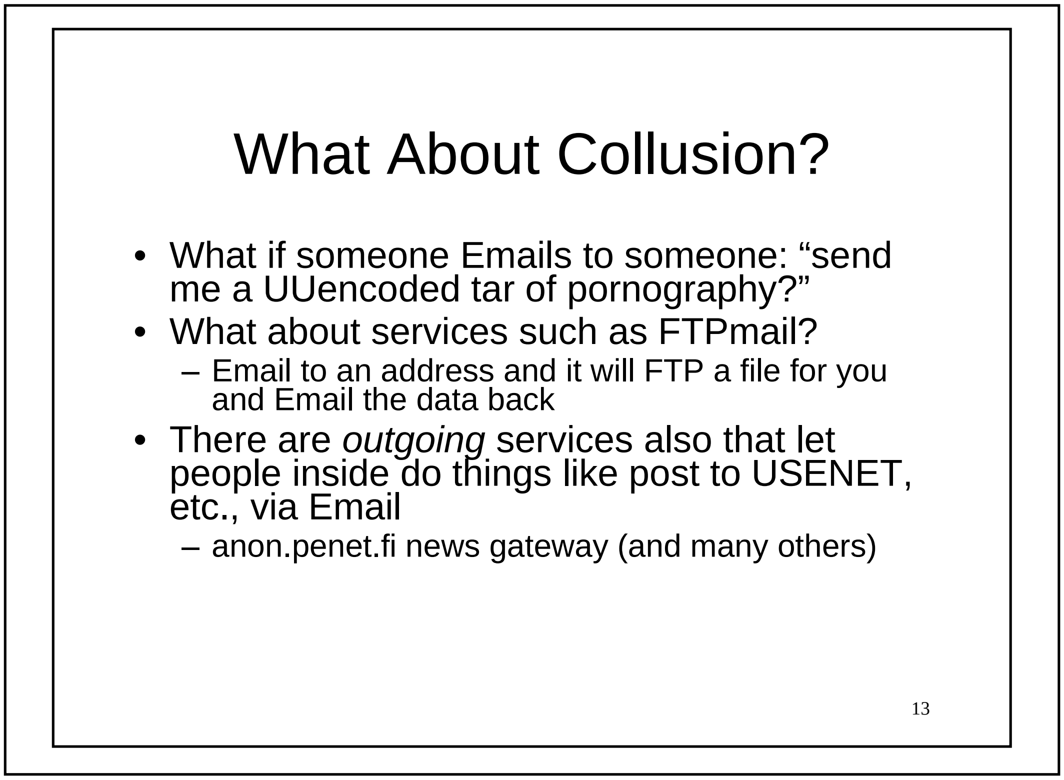
Proactive Censorship

- Requires that you read everything manually
  - And there’s a LOT of content out there!
- Requires some policy for updates to permitted content database
- May be “mistake proof” by being extremely conservative
- If less conservative, mistakes will happen



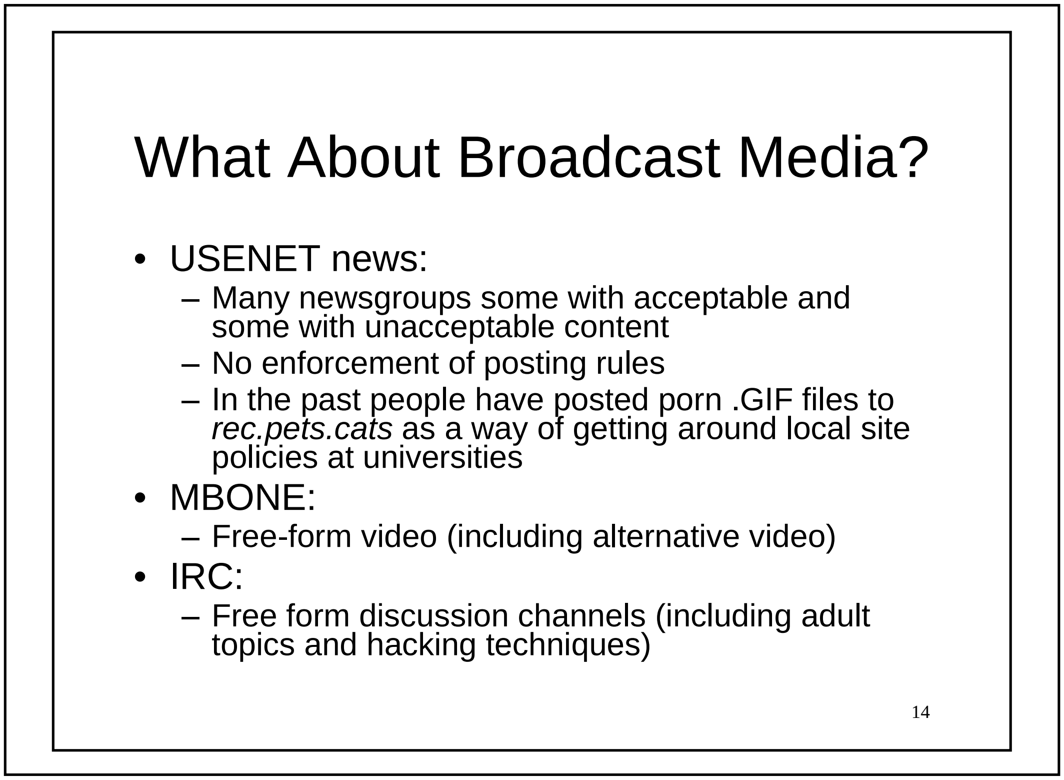
Reactive Censorship

- Perform traffic/size analysis and correlation
  - Search for large image transfers from sites that appear often
  - Flag them for examination
  - If the examination reveals contraband material then shut the site (or URL) off
- Problem:
  - A piece of software cannot distinguish a .GIF image of a sea otter from a .GIF image of a naked human
- Humans still required for observation
- Can use (transparent) non-intrusive monitoring



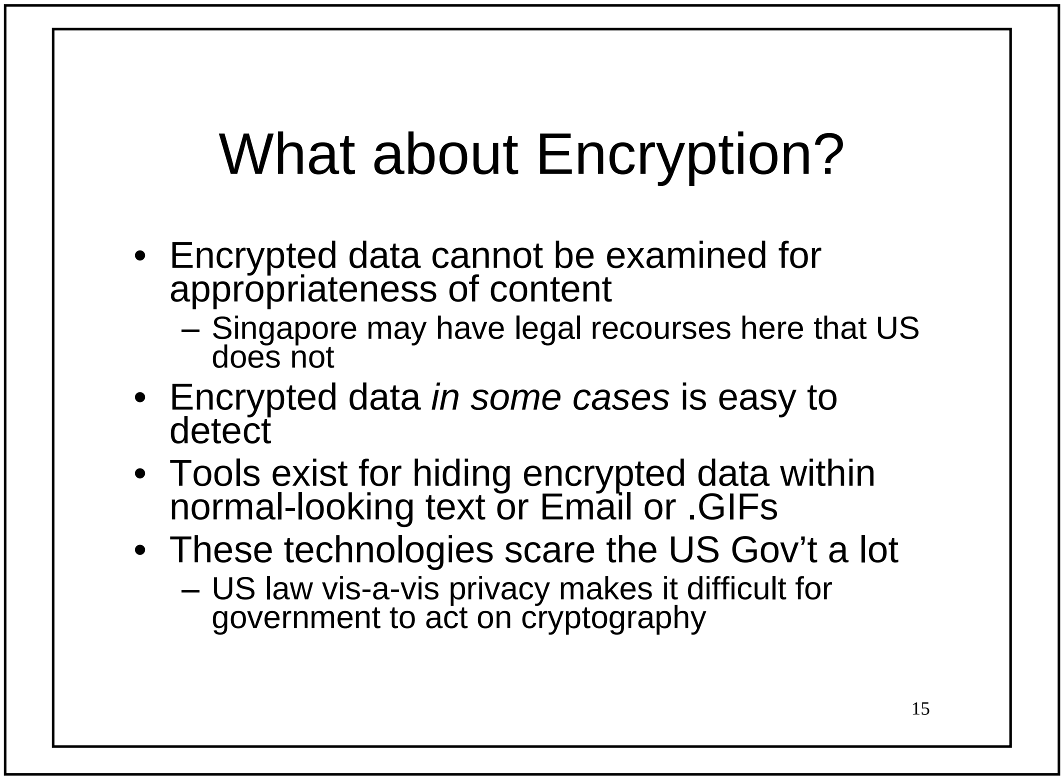
What About Collusion?

- What if someone Emails to someone: “send me a UUencoded tar of pornography?”
- What about services such as FTPmail?
  - Email to an address and it will FTP a file for you and Email the data back
- There are *outgoing* services also that let people inside do things like post to USENET, etc., via Email
  - anon.penet.fi news gateway (and many others)



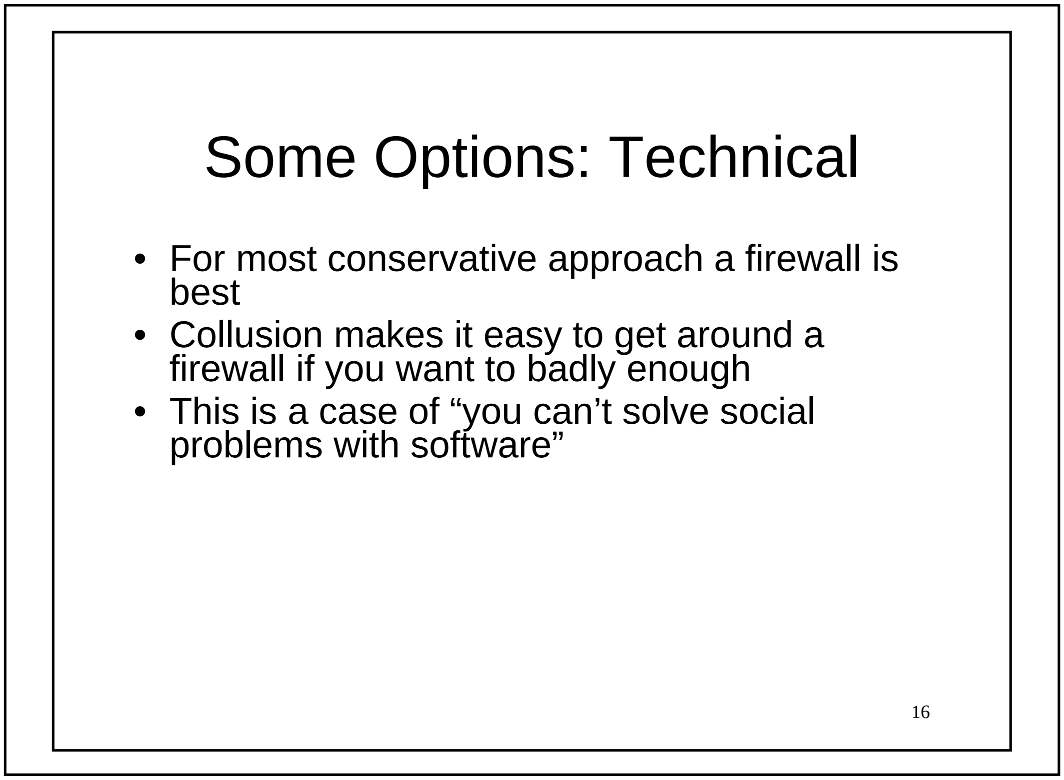
What About Broadcast Media?

- USENET news:
  - Many newsgroups some with acceptable and some with unacceptable content
  - No enforcement of posting rules
  - In the past people have posted porn .GIF files to *rec.pets.cats* as a way of getting around local site policies at universities
- MBONE:
  - Free-form video (including alternative video)
- IRC:
  - Free form discussion channels (including adult topics and hacking techniques)



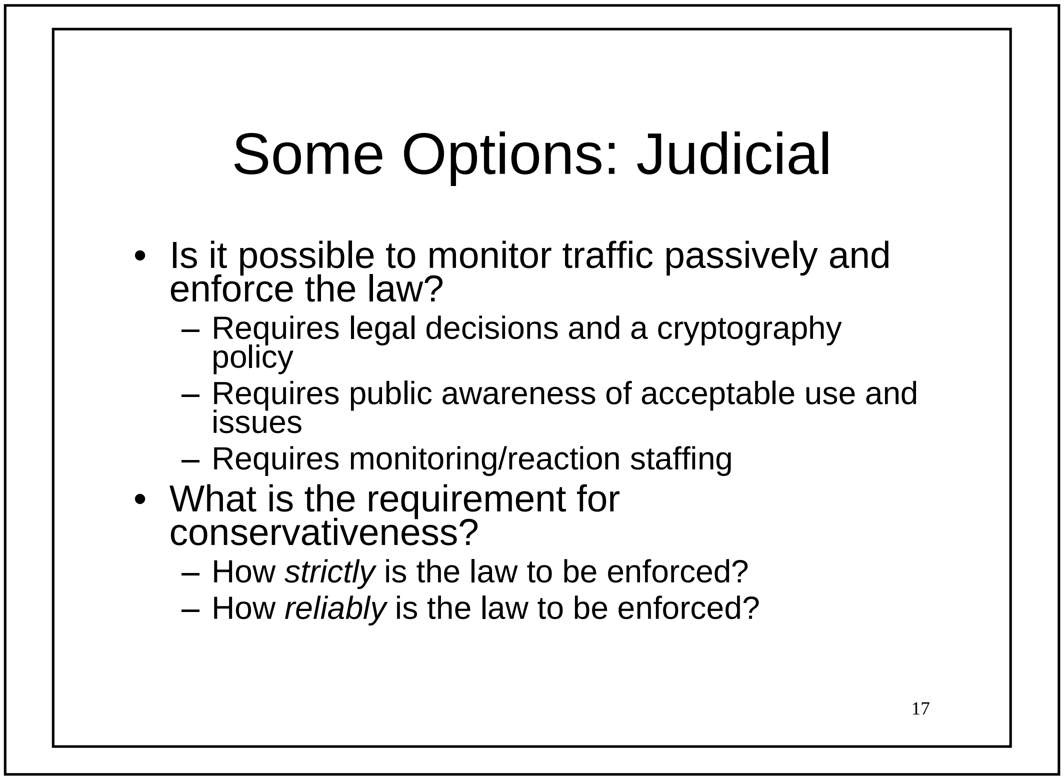
What about Encryption?

- Encrypted data cannot be examined for appropriateness of content
  - Singapore may have legal recourses here that US does not
- Encrypted data *in some cases* is easy to detect
- Tools exist for hiding encrypted data within normal-looking text or Email or .GIFs
- These technologies scare the US Gov't a lot
  - US law vis-a-vis privacy makes it difficult for government to act on cryptography



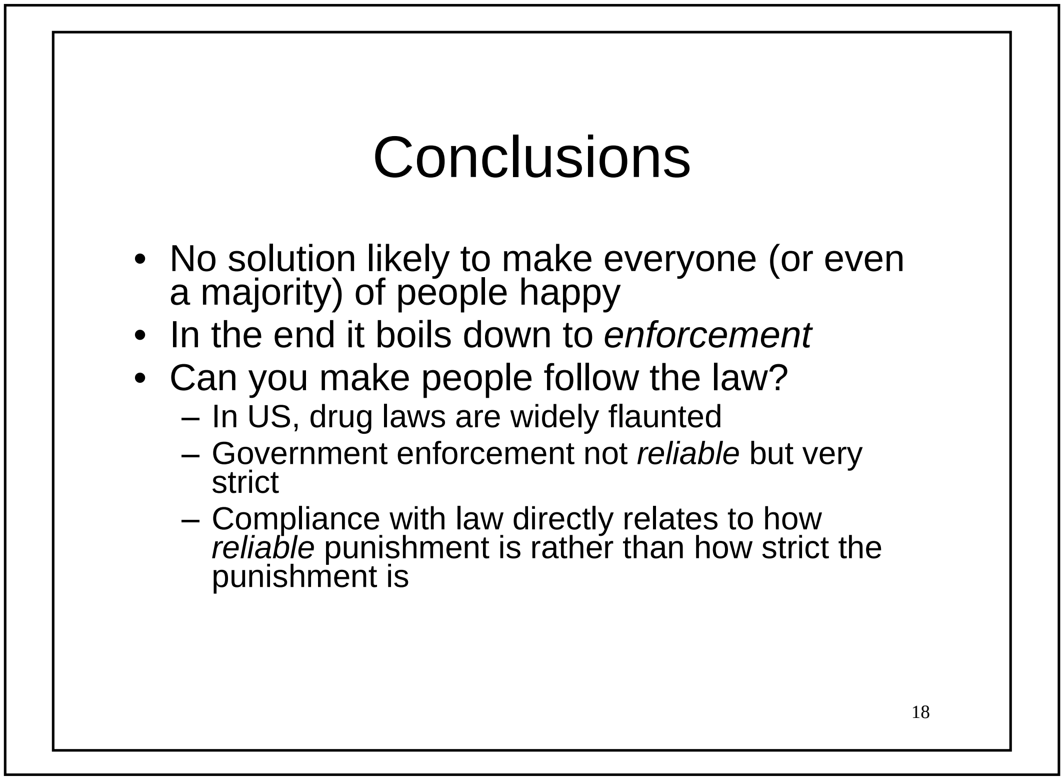
Some Options: Technical

- For most conservative approach a firewall is best
- Collusion makes it easy to get around a firewall if you want to badly enough
- This is a case of "you can't solve social problems with software"



Some Options: Judicial

- Is it possible to monitor traffic passively and enforce the law?
  - Requires legal decisions and a cryptography policy
  - Requires public awareness of acceptable use and issues
  - Requires monitoring/reaction staffing
- What is the requirement for conservativeness?
  - How *strictly* is the law to be enforced?
  - How *reliably* is the law to be enforced?



Conclusions

- No solution likely to make everyone (or even a majority) of people happy
- In the end it boils down to *enforcement*
- Can you make people follow the law?
  - In US, drug laws are widely flaunted
  - Government enforcement not *reliable* but very strict
  - Compliance with law directly relates to how *reliable* punishment is rather than how strict the punishment is