Article 19

“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”

Article 20

“Everyone has the right to freedom of peaceful assembly and association.”
George Orwell was an optimist

“Who controls the past, controls the future: who controls the present controls the past

— George Orwell, Nineteen Eighty Four, 1949

The re-writing of history is now much more efficient than when George Orwell imagined armies of Winston Smiths cutting holes in newspaper archives
Online archives are easily censored
Online archives are easily censored

UK mobile giant seeks £7.5bn Dutch merger
The Observer, Sunday April 6 2003
Jamie Doward, deputy business editor
A management team from mobile phone giant mmO2 has held exploratory talks with counterparts at Dutch telecom operator KPN to create a £7.5 billion pan-European wireless champion. Informed sources stressed that the talks, held within the last two months, were informal and nothing was currently being discussed. However, news that the two sides are contemplating merger (…)

Landlords must rent out empty homes
The Observer, Sunday April 6 2003
Jamie Doward
Given the way in which it has been described, you could be forgiven for thinking one of the central planks of the Government's solution to the housing crisis is the most draconian piece of central planning since the Berlin Wall went up. Deputy Prime Minister John Prescott's plan to force landlords to rent out empty homes - discussed in the Government's Sustainable (…) (…) to turn around blighted communities face a number of obstacles, writes Jamie (…)

Sky wins battle for rolling news audience
The Observer, Sunday April 6 2003
Jamie Doward
Even if, according to the French philosopher Jean Baudrillard, the 1991 Gulf war didn't exist, there can be no such doubts about its successor. Baudrillard's much quoted thesis, famously espoused in the pages of Libération, suggested the first conflict - as seen through the prism of the media - came to be depicted as an unreal, imaginary place, a giant video game to (…) (…) a new appetite for 24-hour news among British viewers, reports Jamie (…)

Ex-Chancellor aids fraud suspect
The Observer, Sunday April 6 2003
Jamie Doward, deputy business editor
Former Chancellor Norman Lamont has used his influence to try to help a billionaire business associate arrested in Switzerland amid allegations that his company defrauded another firm of more than €100 million (£87.7m). Lamont wrote two months ago to give the Swiss authorities a character reference for metals broker Vahid Alaghband, who is one of three (…)
Centralized systems work better: cheaper, more versatile, and more efficient

By eliminating distance, the Internet allows greater centralization

Centralized archiving of physical newspapers is awkward, but online archiving works well

This makes life easier for readers, and censors too

Many libraries are now dropping archiving of paper in favor of electronic subscriptions
The Internet eases publication too

- "The Catholic Orangemen of Togo", by Craig Murray, was dropped by its publisher due to libel threats.
- The lack of support from a publisher and network of book shops would previously be devastating.
- However, the Internet facilitates self-publishing and marketing.
The Catholic Orangemen of Togo”, by Craig Murray, was dropped by its publisher due to libel threats


The lack of support from a publisher and network of book shops would previously be devastating

However, the Internet facilitates self-publishing and marketing
Internet architecture allows censorship

Diagram: China Internet Network Information Center
What is being blocked, and why

- According to the Open Net Initiative, at least 70 countries filter the Internet in some way; from Asia, to Europe, to the Americas.

- The types of material censored varied depending on country, e.g.:
  - Human Rights (blocked in China)
  - Religion (blocked in Saudi Arabia, UAE, Iran, Bahrain)
  - Pornography (blocked in Saudi Arabia, UAE, Iran, Bahrain, Singapore, Burma, ...)

- Other issues censored include: military and militant websites; sex education, alcohol/drugs, music; gay and lesbian websites; news
What is being blocked, and why

- According to the Open Net Initiative, at least 70 countries filter the Internet in some way; from Asia, to Europe, to the Americas.
- The types of material censored varied depending on country, e.g.:
  - Human Rights (blocked in China)
  - Religion (blocked in Saudi Arabia, UAE, Iran, Bahrain)
  - Pornography (blocked in Saudi Arabia, UAE, Iran, Bahrain, Singapore, Burma, ...)
- Other issues censored include: military and militant websites; sex education, alcohol/drugs, music; gay and lesbian websites; news
According to the Open Net Initiative, at least 70 countries filter the Internet in some way; from Asia, to Europe, to the Americas.

The types of material censored varied depending on country, e.g.:

- Human Rights (blocked in China)
- Religion (blocked in Saudi Arabia, UAE, Iran, Bahrain)
- Pornography (blocked in Saudi Arabia, UAE, Iran, Bahrain, Singapore, Burma, . . . )

Other issues censored include: military and militant websites; sex education, alcohol/drugs, music; gay and lesbian websites; news.
Search Engine results are censored

Searching for "Tiananmen Square" on Google.com and Google.cn
Chilling effects: self-censorship through fear, intimidation, and punishment

People can be intimidated into not testing rules through fear of detection and retribution

"I call on Egyptian government officials to take the necessary procedures to protect the Egyptian youth from the spread of subversive religious ideologies among them by permanently shutting down religious institutions in this country."

— Kareem Amer (sentenced to four years of prison in Egypt)
Sweden’s iPRED experience

Aggregate traffic All (Fri Nov 13 12:24:04 2009)

Bits per second

- Incoming Traffic in Bits per second
- Outgoing Traffic in Bits per second

Maximal In: 133.198 G  Maximal Out: 133.222 G
Average In: 87.821 G  Average Out: 88.106 G
Current In: 114.684 G  Current Out: 114.695 G
Our analysis shows that consumers increasingly want to decide for themselves when to watch and from which screen. Unfortunately, many have become adept at circumventing the IPRED legislation.

— Jens Heron, Mediavision
The Net interprets censorship as damage and routes around it.

— John Gilmore, 1993

No longer true on a technical level: censorship is in the routers.

Remains true on a social level: when material is censored, people distribute copies and draw attention to them.

But what if people are too afraid to do this?
United States Constitution: 1st Amendment

“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.”

McIntyre v. Ohio Elections Commission

“Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views... Anonymity is a shield from the tyranny of the majority... It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular”
Twitter in Iran: Good.

Iran Protests: Twitter, the Medium of the Movement

By LEV GROSSMAN  Wednesday, Jun. 17, 2009

Behind the Scenes with Mousavi

Stories

- In Iran, Rival Regime Factions Play a High-Stakes Game of Chicken
- Latest Tweets on Fallout from Iran's

The U.S. State Department doesn't usually take an interest in the maintenance schedules of dotcom start-ups. But over the weekend, officials there reached out to Twitter and asked them to delay a network upgrade that was scheduled for Monday night. The reason? To protect the interests of...
FBI Raids Queens Home in G20 Protest Twitter Crackdown

That's right, a Twitter crackdown. A lawyer for Jackson Heights social worker Elliot Madison, 41, says that the feds searched his client's house for 16 hours on Thursday after Madison was arrested on September 24th at a Pittsburgh hotel room with another man. What were they up to? Sitting at laptops sending Twitter messages advising G20 demonstrators about riot police activity in the streets. And yet real Twitter threats like Lindsay Lohan and Courtney Love remain at large.

Madison, a self-described anarchist, was in Pittsburgh volunteering for the Tin Can Comms Collective, a group that uses Twitter to send mass text messages during protests describing events observed on the streets or over police scanners; stuff like "SWAT teams rolling down 5th Ave." Tin Can was active during the St. Paul RNC protests, and the authorities are now on to them. Madison was charged with hindering apprehension or prosecution, criminal use of a communication facility and possession of instruments of crime; he's currently out on bail.

from http://gothamist.com/2009/10/05/fbi_raids_queens_home_in_g20_protes.php
Internet surveillance is pervasive

- Conventional surveillance methods had to be targeted
- Internet censorship is capable of monitoring everyone, all of the time
- Governments are increasing monitoring: SORM (Russia), Golden Shield (China), Data Retention Directive (EU), and Interception Modernisation Programme (UK), Warrantless Wiretapping (USA)
- 1 in 7 East German citizens worked for the Stasi. Today we can achieve the same results with a fraction of the cost
Traffic data surveillance

- Traffic data (who talks to whom, how often and for how long) is the core of intelligence capabilities
- This information is cheaper to record and store, compared to full content
- Because it can be easily processed by computer, data mining techniques can be used to understand social structures

“No government of any colour is to be trusted with such a roadmap to our souls”

— Sir Ken Macdonald, former director of public prosecutions, on the UK Interception Modernisation Program
Importantly, information on social networks can be derived from:

- Communities
- People

From "The Economics of Mass Surveillance" by George Danezis and Bettina Wittneben
• David Brin proposed that in a world of pervasive surveillance, balance could be maintained by allowing everyone to monitor everyone else

• Bruce Schneier retorted that surveillance amplifies existing powers

• Many countries restrict anonymous speech (e.g. Germany and China)

• It is easy for those in power to call on the weak to link their names to opinions
Censorship resistance systems

- Software to resist censorship should
  - have a diverse set of users
  - work where you are without special steps
  - be sustainable (what if the company goes broke?)
  - be decentralized (swapping censors doesn’t help you)
  - protect you by default
  - have accessible standards and published designs (black box vs. glass box)
  - be fast enough that you’ll use it daily
  - doesn’t promise perfect everything including a fully encrypted Internet

- These properties should be maintained even if the censorship resistance system is partially compromised
• When a country’s government controls international connectivity, they can block requests for banned websites and destinations
• There are a number of different approaches (DNS blocking, IP address blocking, etc.)
• Software may be produced in-country, but often is an adapted commercial product
• These companies not only make the software, but provide a continuously updated list of websites to be blocked
Normal web browsing

1. User requests www.example.org/page.html
2. DNS lookup for www.example.org
3. Lookup response: www.example.org is 192.0.2.166
4. www.example.org is 192.0.2.166
5. Get web page: www.example.org/page.html at 192.0.2.166
6. Here is www.example.org/page.html

Diagram: Jane Gowan
DNS tampering

1. User requests www.example.org/page.html
2. DNS response: www.example.org does not exist

Diagram: Jane Gowen
1. User requests www.example.org/page.html
2. DNS lookup for www.example.org
3. Lookup response: www.example.org is 192.0.2.166
4. www.example.org is 192.0.2.166
5. Get web page: www.example.org/page.html at 192.0.2.166
6. Router drops all packets to 192.0.2.166
7. Browser concludes that www.example.org is inaccessible
Trade-offs in blocking systems

- DNS blocking
  - Easy and cheap to implement
  - Blocks at domain name granularity – over blocks protocols, web pages
  - Trivial to bypass

- IP blocking
  - Easy and cheap to implement
  - Blocks at IP address (perhaps port) – over blocks virtual hosting

- Proxy blocking
  - Expensive to implement
  - Blocks at webpage level – low over-blocking

- Hybrid blocking – IP based redirection to proxy
  - Tricky to get right, but cheap
  - Has some vulnerabilities
  - Blocks at webpage level – low over-blocking
Trade-offs in blocking systems

- **DNS blocking**
  - Easy and cheap to implement
  - Blocks at domain name granularity – over blocks protocols, web pages
  - Trivial to bypass

- **IP blocking**
  - Easy and cheap to implement
  - Blocks at IP address (perhaps port) – over-blocks virtual hosting
Trade-offs in blocking systems

- DNS blocking
  - Easy and cheap to implement
  - Blocks at domain name granularity – over blocks protocols, web pages
  - Trivial to bypass

- IP blocking
  - Easy and cheap to implement
  - Blocks at IP address (perhaps port) – over-blocks virtual hosting

- Proxy blocking
  - Expensive to implement
  - Blocks at webpage level – low over-blocking
Trade-offs in blocking systems

- **DNS blocking**
  - Easy and cheap to implement
  - Blocks at domain name granularity – over blocks protocols, web pages
  - Trivial to bypass
- **IP blocking**
  - Easy and cheap to implement
  - Blocks at IP address (perhaps port) – over-blocks virtual hosting
- **Proxy blocking**
  - Expensive to implement
  - Blocks at webpage level – low over-blocking
- **Hybrid blocking – IP based redirection to proxy**
  - Tricky to get right, but cheap
  - Has some vulnerabilities
  - Blocks at webpage level – low over-blocking
Who wants online privacy?

- Ordinary people
  - To avoid personal information being sold to marketers
  - Protect themselves when researching sensitive topics

- Military and Law Enforcement
  - To carry out intelligence gathering
  - Protect undercover field agents
  - Offer anonymous tip lines

- Journalists
  - To protect sources, such as whistle blowers

- Human rights workers
  - To publicize abuses and protect themselves from surveillance
  - Blogging about controversial subjects

- Businesses
  - To observe their competition and build anonymous collaborations
Who wants online privacy?

- Ordinary people
  - To avoid personal information being sold to marketers
  - Protect themselves when researching sensitive topics

- Military and Law Enforcement
  - To carry out intelligence gathering
  - Protect undercover field agents
  - Offer anonymous tip lines

- Journalists
  - To protect sources, such as whistle blowers

- Human rights workers
  - To publicize abuses and protect themselves from surveillance
  - Blogging about controversial subjects

- Businesses
  - To observe their competition and build anonymous collaborations
Who wants online privacy?

- Ordinary people
  - To avoid personal information being sold to marketers
  - Protect themselves when researching sensitive topics
- Military and Law Enforcement
  - To carry out intelligence gathering
  - Protect undercover field agents
  - Offer anonymous tip lines
- Journalists
  - To protect sources, such as whistle blowers
Who wants online privacy?

- Ordinary people
  - To avoid personal information being sold to marketers
  - Protect themselves when researching sensitive topics
- Military and Law Enforcement
  - To carry out intelligence gathering
  - Protect undercover field agents
  - Offer anonymous tip lines
- Journalists
  - To protect sources, such as whistle blowers
- Human rights workers
  - To publicize abuses and protect themselves from surveillance
  - Blogging about controversial subjects
Who wants online privacy?

• Ordinary people
  • To avoid personal information being sold to marketers
  • Protect themselves when researching sensitive topics

• Military and Law Enforcement
  • To carry out intelligence gathering
  • Protect undercover field agents
  • Offer anonymous tip lines

• Journalists
  • To protect sources, such as whistle blowers

• Human rights workers
  • To publicize abuses and protect themselves from surveillance
  • Blogging about controversial subjects

• Businesses
  • To observe their competition and build anonymous collaborations
Anonymous communication

- People have to hide in a crowd of other people ("anonymity loves company")
- The goal of the system is to make all users look as similar as possible, to give a bigger crowd
- Hide who is communicating with whom
- Layered encryption and random delays hide correlation between input traffic and output traffic
Tor is a low-latency anonymity system

- Based on technology developed in the Onion Routing project
- Privacy by design, not by policy (no data collected)
- Commonly used for web browsing and instant messaging (works for any TCP traffic)
- Originally built as a pure anonymity system (hides who is talking to whom)
- Now designed to resist censorship too (hides whether someone is using the system at all)
- Centralized directory authorities publish a list of all servers; client doesn’t trust the network by design
Tor is a low-latency anonymity system

- Based on technology developed in the Onion Routing project
- Privacy by design, not by policy (no data collected)
Tor is a low-latency anonymity system

- Based on technology developed in the Onion Routing project
- Privacy by design, not by policy (no data collected)
- Commonly used for web browsing and instant messaging (works for any TCP traffic)
Tor is a low-latency anonymity system

- Based on technology developed in the Onion Routing project
- Privacy by design, not by policy (no data collected)
- Commonly used for web browsing and instant messaging (works for any TCP traffic)
- Originally built as a pure anonymity system (hides who is talking to whom)
Tor is a low-latency anonymity system

- Based on technology developed in the Onion Routing project
- Privacy by design, not by policy (no data collected)
- Commonly used for web browsing and instant messaging (works for any TCP traffic)
- Originally built as a pure anonymity system (hides who is talking to whom)
- Now designed to resist censorship too (hides whether someone is using the system at all)
Tor is a low-latency anonymity system

- Based on technology developed in the Onion Routing project
- Privacy by design, not by policy (no data collected)
- Commonly used for web browsing and instant messaging (works for any TCP traffic)
- Originally built as a pure anonymity system (hides who is talking to whom)
- Now designed to resist censorship too (hides whether someone is using the system at all)
- Centralized directory authorities publish a list of all servers; client doesn’t trust the network by design
Tor hides communication patterns by relaying data through volunteer servers.
Tor hides communication patterns by relaying data through volunteer servers.
Tor hides communication patterns by relaying data through volunteer servers.

Diagram: Robert Watson
Tor hidden services allow censorship resistant services.
How is Tor different from other systems?
How is Tor different from other systems?
How is Tor different from other systems?
Limitations of censorship resistance

- Censorship resistance is thought controversial – especially by the censors
- There is something for everyone to like, and something for everyone to dislike, going on with censorship resistance systems
- Bad people do use them to do bad things (for many different definitions of bad people)
- It is impossible to block bad uses, even if we could come up with a common definition of bad content
- The systems are not perfect, so it is possible some people will be caught
Conclusions

• The Internet and centralisation can both improve and harm freedom of speech

• Slogans regarding the borderless nature and inherent freedoms of the Internet are frequently wrong

• Technical details matter: how a system is implemented can make a radical difference

• Technologies can be used to resist censorship and improve privacy

• However, policies must be changed too and pressure is needed on legislators
I’d like to change the design of the Internet by introducing regulation–Internet passports, Internet police and international agreement–about following Internet standards. And if some countries don’t agree with or don’t pay attention to the agreement, just cut them off.

— Eugene Kaspersky, Co-Founder & CEO of Kaspersky Labs
Internet Access as a Human Right

“*We think it’s something you cannot live without in modern society. Like banking services or water or electricity, you need an Internet connection.*

— Laura Vilkkonen, Ministry of Transport and Communications, Finland

Tor Project’s Mission

“We remain committed to defending online privacy and anonymity as a human right.”
How to get there

- Increased funding of research and development for privacy, circumvention, and anti-censorship technologies
- Policy and Legal frameworks for free access, free speech, and anonymity
• Thank you to Steven J. Murdoch, http://www.cl.cam.ac.uk/users/sjm217/, for the research and basis for this presentation.

• Photographer and Diagram credits as listed throughout the presentation.