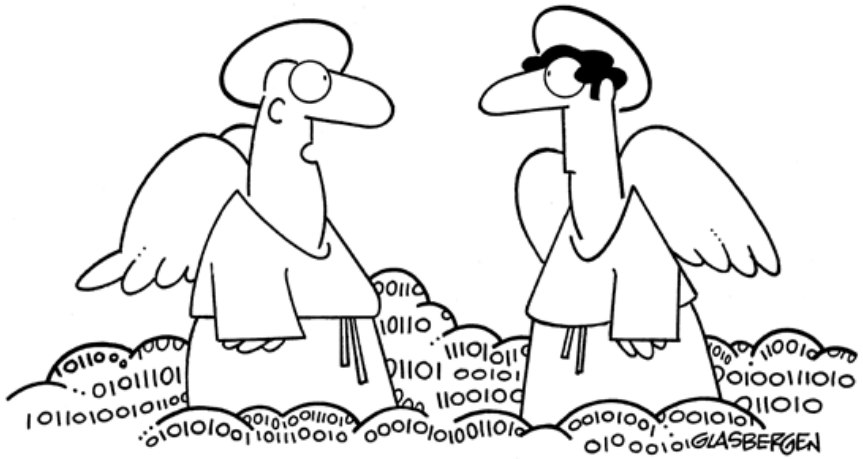
Ethical, Social and Legal Issues on the Web

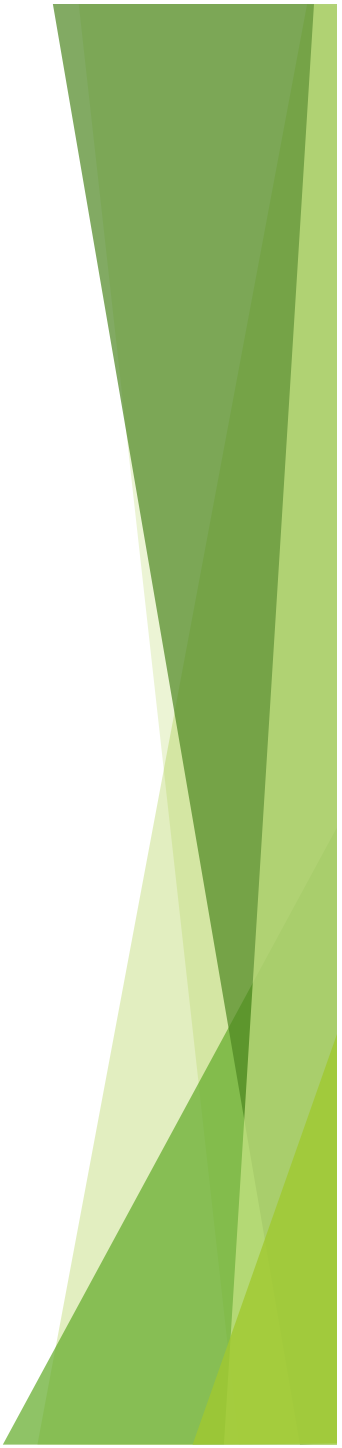
Lecture 8 – COMPSCI111/111G



"You should have been here back in the old days before cloud computing."

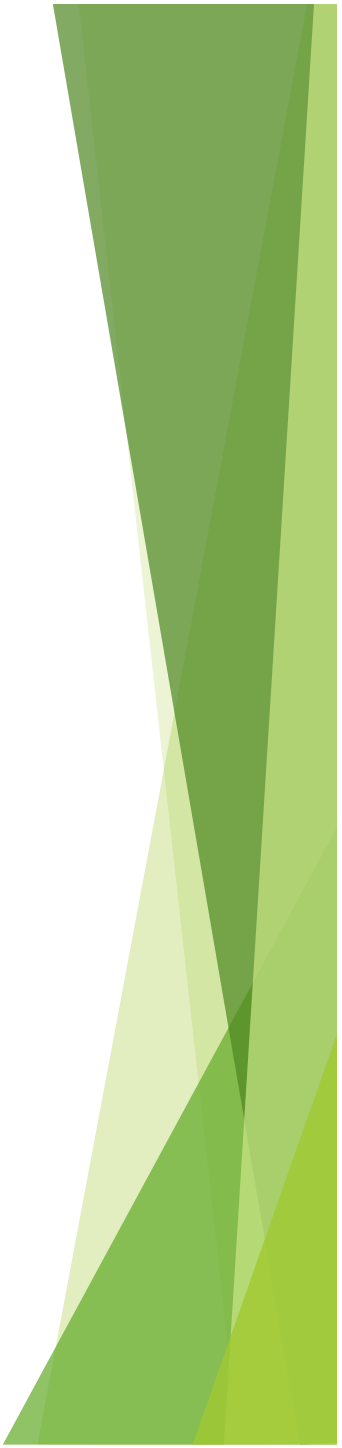
Recap

- We've already discussed a number of social issues:
  - L5- electronic communication:
    - Spam
    - Misrepresentation online
  - L6- publishing online:
    - Reliability of information on Wikipedia
  - L7- the World Wide Web:
    - Search engines and the implications of their data collection



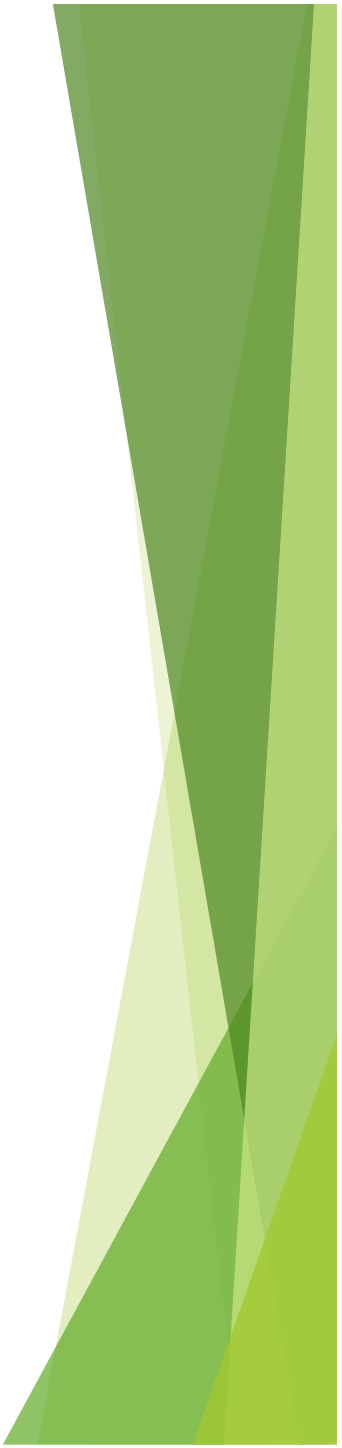
Today's lecture

- Ethical
  - Online anonymity
  - Different kinds of malware
- Social
  - Online bullying
  - Cultural dominance
- Legal
  - Copyright and file sharing
  - Censorship on the Web



Ethical issues

Online anonymity, malware



Online anonymity

- It is impossible to be completely anonymous on the Web
- However, it is possible to remain fairly anonymous on the Internet
  - Used to be difficult to associate an IP address with a person's computer
  - Easy to give fake information when creating an account on a website
  - Most websites don't perform an ID check on their users

Online anonymity

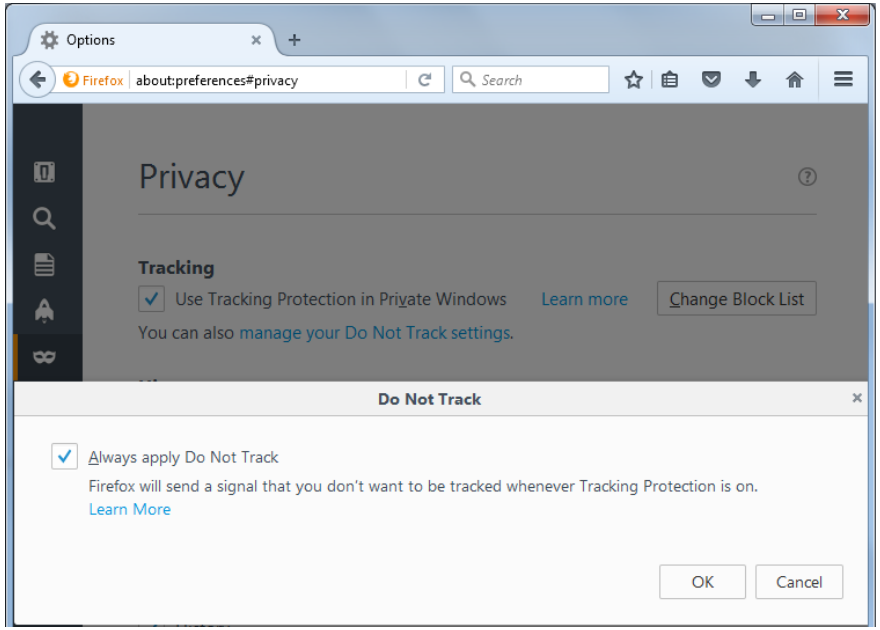
- Anonymity on the Internet is being eroded:
  - Advertisers are able to effectively track users' preferences and browsing habits
    - Eg. fingerprinting computers better than using cookies
  - Websites demand more personal information and keep track of users' activities
  - Laws require ISPs to keep a record of the IP addresses assigned to users
  - Governments are expanding their online surveillance powers

Online anonymity

- Advantages:
  - Encourages free expression online, especially around sensitive or personal issues
  - Supports other rights such as the right to privacy
- Disadvantages:
  - Use of anonymity to harass and offend other people
    - Eg. ‘trolls’ on Twitter
  - Difficult to authenticate whether a message (eg. email) is from the purported sender
  - Makes it difficult for authorities to track criminal activity online

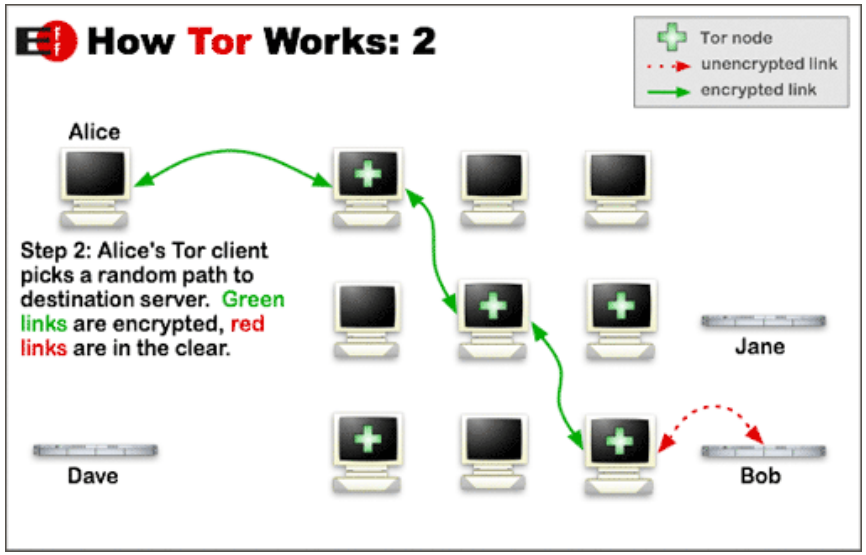
Online anonymity

- Do Not Track initiative:
  - A browser option that tells an advertiser you do not want them to track your browsing habits
  - Voluntary system; the advertiser is under no obligation to abide by Do Not Track requests
  - Potential solution to the creation of filter bubbles?



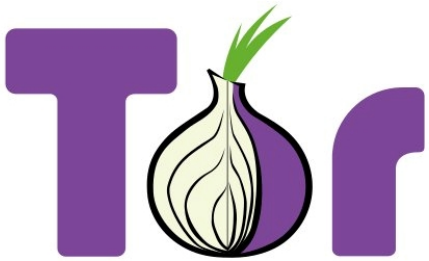
Online anonymity

- The Tor Project:
  - A network of servers that use **onion routing** to obscure the path that packets take when moving from sender to receiver
    - Onion routing involves sending the packet along a random path through a set of encrypted relays
  - Need to use the Tor browser in order to browse the Web over the Tor network



Online anonymity

- By protecting data as it is being transported, Tor makes it difficult to intercept data or find the source/destination
- However, it doesn't protect a user's computer from cookies or from being fingerprinted
- While the extra anonymity provided by Tor is useful, it has also been misused (eg. the Silk Road)

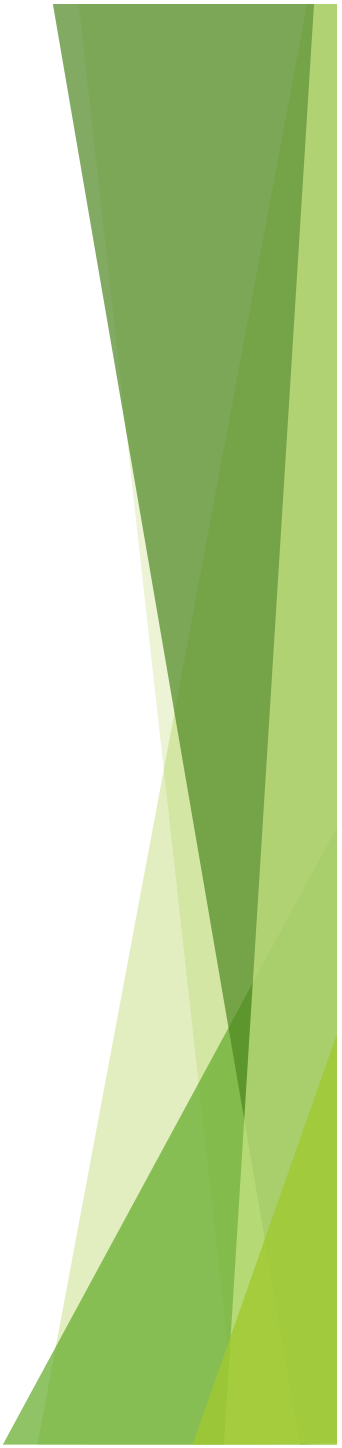


Malware

- **Malware:** malicious software, which includes:
  - **Viruses:** inserts itself into another program; runs and spreads itself when the program is opened (eg. macro viruses)
  - **Worms:** similar to viruses except they don't need a program in order to run; spreads by itself (eg. Stuxnet)
  - **Trojans:** malware disguised as legitimate software that allow people to access your computer (eg. Koobface)
  - **Spyware:** runs in the background, monitoring the user's activities and sending the info back to the operator (eg. keyloggers)
  - **Logic bombs:** malware deliberately inserted into a program which runs when a certain condition is fulfilled (eg. the Roger Duronio case)

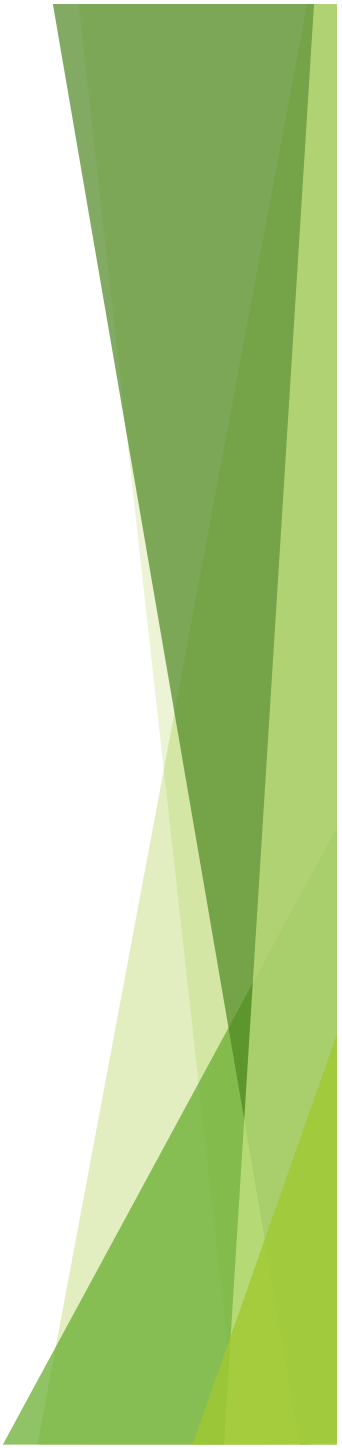
Malware

- The best protection against malware is a good anti-virus program and the use of safe browsing practices:
  - Don’t click on unknown links
  - Delete spam messages
  - Don’t open unknown attachments



Social issues

Online bullying, cultural dominance



Online bullying

- Some people take advantage of online anonymity to bully and harass others online
- One UoA study found 11.5% of people in NZ over 18 have experienced online bullying
- Online bullying is a growing problem among youth. Our ‘always online’ society makes it difficult to avoid online bullying

Online bullying

- The Harmful Digital Communications Act 2015 (HDCA) is one response to this growing problem
  - s3: purpose of this Act is to:
    - Deter and mitigate harm caused by digital communications
    - Provide redress to victims of harmful digital communications
- s4: key definitions
  - 'digital communication' means "any form of electronic communication" – includes texts, emails, IM, forum posts, Snapchat etc.
  - 'harm' means "serious emotional distress"
- Two main avenues of redress under the HDCA

Online bullying

- **First option:** complain to the Approved Agency
  - Approved Agency is Netsafe; a non-profit organization
- If the complaint is genuine, Netsafe will use "negotiation, mediation, and persuasion (as appropriate) to resolve complaints" – s8(1)(c)
- s11: after Netsafe has assessed the complaint, the person can apply to the District Court for an order
  - s12: Court must be satisfied that the communications principles have been breached (s6) and that the person has been harmed
  - Orders under sections 18 and 19 include:
    - Take down material, cease conduct, publish a correction, publish an apology

Online bullying

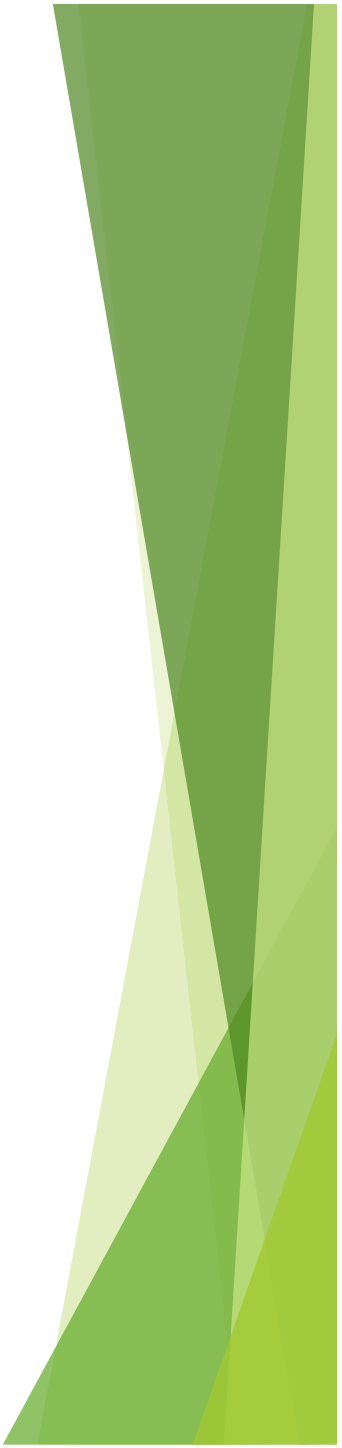
- **Second option:** person or Netsafe can complain to online content host (a person who controls "an electronic retrieval system") where the harmful digital communication can be accessed
  - Includes social media sites, blogs, search engines
- s24: when a host gets a complaint, it must try to contact the author of the harmful digital comm.
  - If the author responds and refuses to remove the material, then the host can't do anything
  - If author doesn't respond or the author agrees, the host must take down the content within 48 hours
- s23: following this process protects the online content host from any legal liability arising from the harmful digital communication

Cultural dominance

- The Internet was popularised in the USA and English is the dominant language online
- Other cultures now have a strong presence and influence on the Web
  - Chinese social media platforms, eg. Weibo, Wechat
  - K-pop
- Diverse control over key pieces of Internet infrastructure. Examples:
  - We've seen backbone cables are mostly owned by private companies
  - ICANN now manages the DNS system (news article)

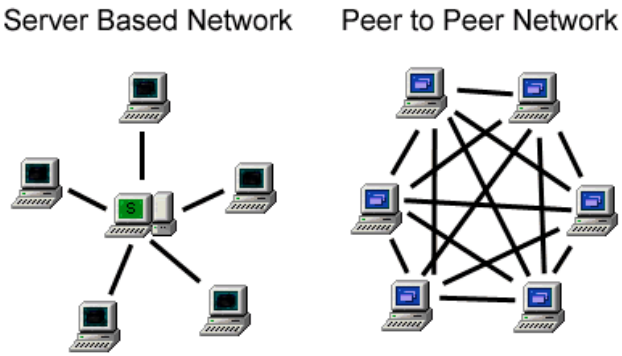
Legal issues

Copyright and file sharing, censorship on the Web



File sharing

- One of the Web's main aims was to help people easily share information
- Today, cloud storage (eg. Dropbox, Google Drive) is an easy way of storing and sharing files
- Peer-to-peer (P2P) networks provide another way of sharing files
  - P2P networks use the BitTorrent protocol to enable computers to connect to each other and share data

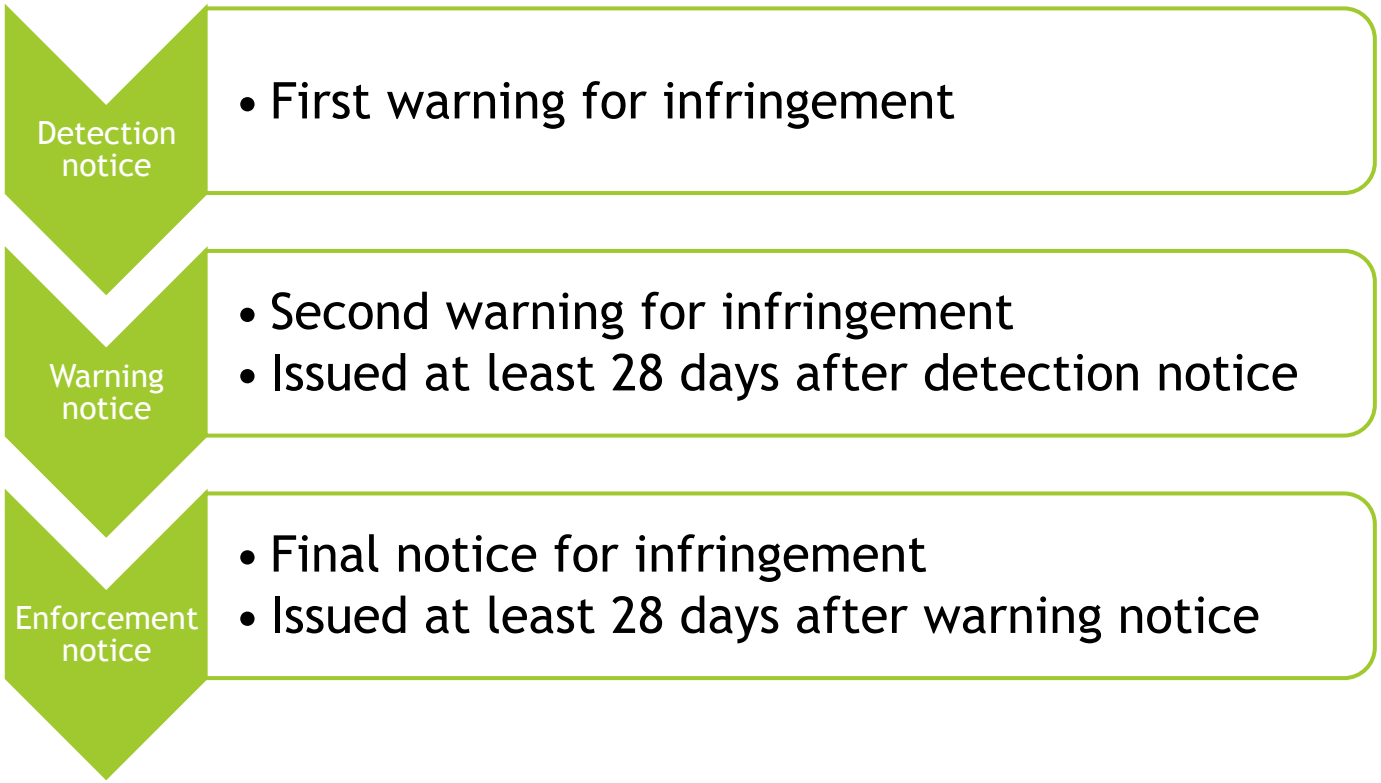


File sharing

- Unfortunately file sharing on P2P networks is used for copyright infringement
  - Copyright protects an author's work from being copied without their permission
  - One of the most famous P2P networks is The Pirate Bay
- The Copyright Act 1994, sections 122A to 122U, provides a way for copyright holders to complain about file sharing on P2P networks

File sharing

- Up to three notices are given to the infringer by their ISP in a nine month period
- Infringer can challenge each notice



File sharing

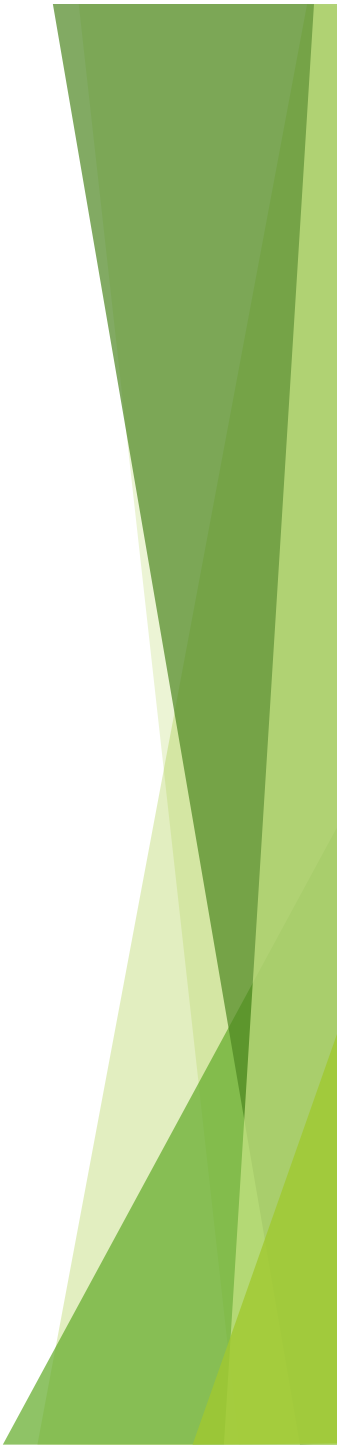
- When an enforcement notice is issued, the infringer can be penalised:
  - Copyright Tribunal can impose a penalty of up to $15,000
    - Example of a decision by the Tribunal
  - District Court can suspend the infringer's Internet connection for up to 6 months

Censorship on the Web

- The Office of Film and Literature Classification is responsible for determining the age classification of publications
  - Includes movies, books, games, clothing, pictures, computer files etc.
- Three levels of classification:
  - **G, PG, M:** publication can be viewed by anyone, caution needed around PG and M
  - **R13, R15, R16, R18:** publication can **only** be viewed by people of the given age and over
  - **RP13, RP16:** publication can **only** be viewed by people of the given age and under if **accompanied** by their parent

Censorship on the Web

- Any publication on the Web (movies, games, music etc) is subject to NZ's censorship laws when accessible in NZ
  - So movies and games sold online must have a classification label if required
  - Sometimes, a publication is classified as objectionable, meaning it can't be owned or sold in NZ
    - Objectionable publications are those with extremely sexual, violent or offensive content



Censorship on the Web

- Software can help to restrict access to certain content on the Web
- Blocking software
  - Uses a blacklist or whitelist of IP addresses to determine which websites can be accessed and which websites should be blocked
  - Eg. Department of Internal Affairs DCEFS
- Web filter
  - Prevents access to websites based on their content (eg. image/video screening, keywords, malware etc)
  - Eg. K9 web filter, tutorial for running a filter on a proxy

Questions

- What is the main weakness of the Do Not Track initiative?
- What is the key difference between a virus and a worm?
- Name one of the orders that a court can make under the Harmful Digital Communications Act
- What are the differences between the R13 and the RP13 classification?

Answers

- What is the main weakness of the Do Not Track initiative?
  - It is voluntary, so advertisers can choose to ignore a Do Not Track setting
- What is the key difference between a virus and a worm?
  - A virus needs a host program in order to run and spread but a worm can run and spread without needing a host program

Answers

- Name one of the orders a court can make under the Harmful Digital Communications Act
  - Any of: take down harmful material, cease harmful conduct, publish a correction, publish an apology
- What are the differences between the R13 and the RP13 classification?
  - R13: publication only viewable to persons 13 and over
  - RP13: publication only viewable to persons 13 and over if accompanied by a parent or guardian

More Exercises

- John downloads a media player application. Shortly after starting the application he discovers that all of his documents are deleted. What sort of malware has John downloaded?
- Worm
- Trojan
- Logic bomb
- Virus
- Spyware

More Exercises

- John downloads a media player application. Shortly after starting the application he discovers that all of his documents are deleted. What sort of malware has John downloaded?
- Worm
- Trojan
- Logic bomb
- Virus
- Spyware

Another question

- Lisa is being harassed by one of her classmate online. What options does she have to address this under the Harmful Digital Communications Act of 2015?

1. She can send harmful messages back to her harasser in order to stop their bullying.
2. She can lodge a complaint with Netsafe.
3. She can apply to the District Court for an order.
4. She can lodge a complaint to the online content host where the harmful messages can be accessed.
5. She can lodge a police report against her harasser.

Another question

- Lisa is being harassed by one of her classmate online. What options does she have to address this under the Harmful Digital Communications Act of 2015?

1. She can send harmful messages back to her harasser in order to stop their bullying.
2. She can lodge a complaint with Netsafe.
3. She can apply to the District Court for an order.
4. She can lodge a complaint to the online content host where the harmful messages can be accessed.
5. She can lodge a police report against her harasser.

Summary

- Ethical
  - Online anonymity is eroding but can still be protected
  - Malware includes viruses, worms, spyware, Trojan horses and logic bombs
- Social
  - Online bullying and the Harmful Digital Communications Act
  - Cultural dominance
- Legal
  - Copyright Act 1994 and file sharing
  - Censorship on the Web through classifications and web filtering