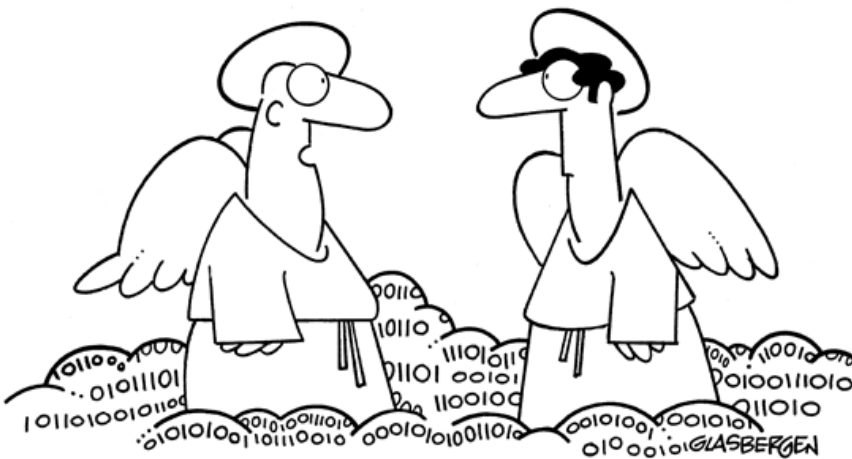# Ethical, Social and Legal Issues on the Web

Lecture 8 – COMPSCI111/111G

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

Major issues

- Unintentional? harm to society
  - How data analysis can impact our society
  - Online anonymity

- Deliberate harm to others
  - Different kinds of malware
  - Online bullying

- Legal constraints
  - Copyright and file sharing
  - Censorship on the Web

Modelling Users

▶ A *vast* amount of data on individuals is being tracked – not just browsing habits, but social media posts, GPS location, loyalty cards, online shopping, and even photos

▶ This data is used to generate very accurate models of individual users – and the more you use devices, the more accurate the model becomes.

▶ The models are so good that many people believe that phones are secretly listening to conversations

▶ https://newatlas.com/computers/facebook-not-secretly-listening-conversations/

Microtargeting

- Using information to divide an audience into specific subgroups and target that group with advertising
  - https://en.wikipedia.org/wiki/Microtargeting
  - https://www.youtube.com/watch?v=cJ5i53b-g6Q

- Cambridge Analytica
  - Company that used microtargeting for political campaigns
  - https://www.youtube.com/watch?v=n8Dd5aVXLCc
  - Found to have harvested Facebook data without permission
  - https://www.youtube.com/watch?v=FXdYSQ6nu-M
  - https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/

Unethical use of data?

▶ Facebook conducted experiments with users by adjusting their new feeds. No consent obtained.

▶ Reducing "positive" posts from friends, resulted in the user posting fewer positive posts

▶ Reducing "negative" posts from friends, resulted in the user posting fewer negative posts

▶ "Emotional contagion" – ability to manipulate the mood of a user.

   ▶ https://www.pnas.org/content/111/24/8788.full
   ▶ https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds

Fake news

▶ Microtargeting and Data Science allows us to segment society and predict what people will react to.

▶ One strategy to influence public opinion is to create news stories that will resonate with the audience and generate the right emotional impact, regardless of the accuracy of the facts.

▶ https://www.journalism.org/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/

▶ https://www.technologyreview.com/s/610635/fake-news-20-personalized-optimized-and-even-harder-to-stop/

▶ https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy

Online anonymity

▶ It is impossible to be completely anonymous on the Web

▶ However, it is possible to remain fairly anonymous on the Internet if you try
  ▶ 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
    ▶ Cookies
    ▶ Fingerprinting (see https://amiunique.org/fp)
    ▶ https://en.wikipedia.org/wiki/Device_fingerprint
  ▶ 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
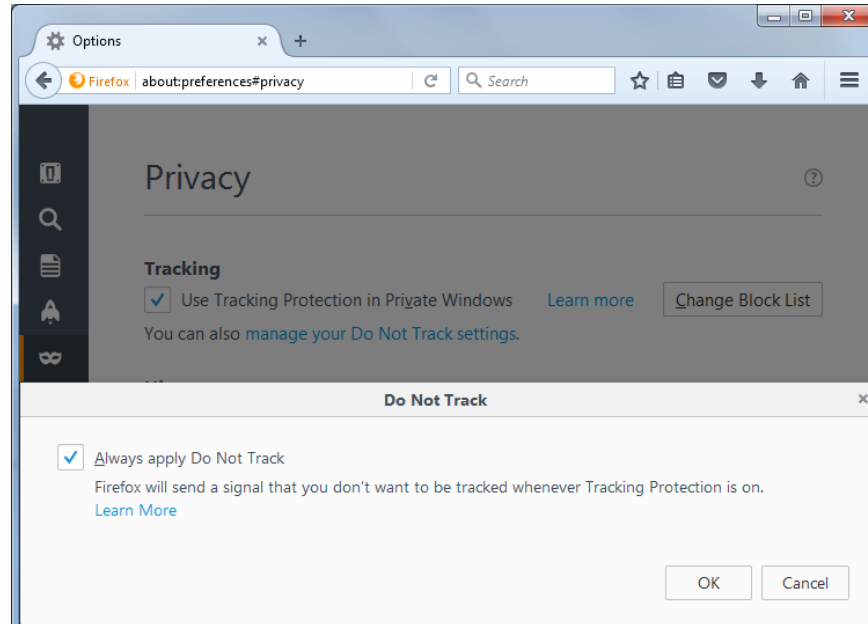
Online anonymity

- 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

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
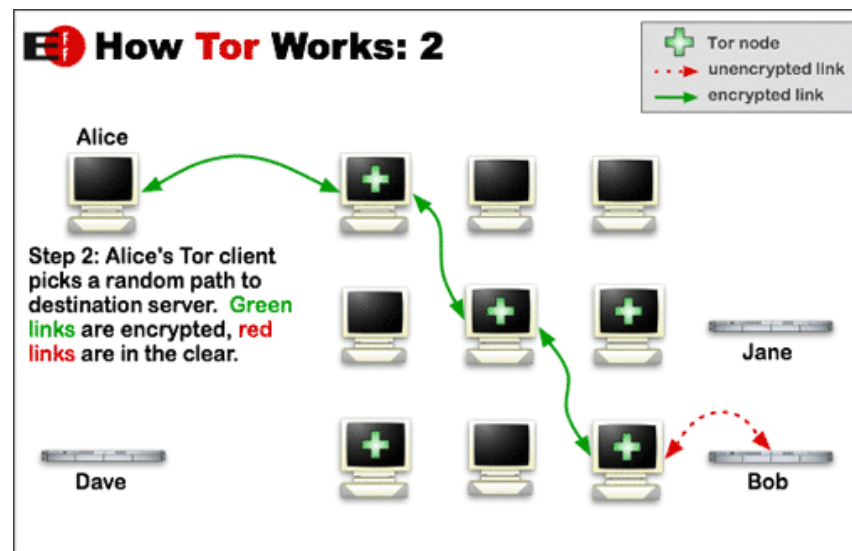
Legal issues

- Deliberate damage – Malware

- Online bullying

- Copyright and file sharing

- Censorship on the Web

Malware

- **Malware:** malicious software, which includes:
    - **Viruses:** inserts itself into another program; runs and spreads itself when the program is opened.
    - **Worms:** similar to viruses except they don't need a program in order to run; spreads by itself.
    - **Trojans:** malware disguised as legitimate software.
    - **Spyware:** runs in the background, monitoring the user's activities and sending the info back to the operator.
    - **Logic bombs:** malware deliberately inserted into a program which runs when a certain condition is fulfilled.

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

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 <u>Netsafe</u>; 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:
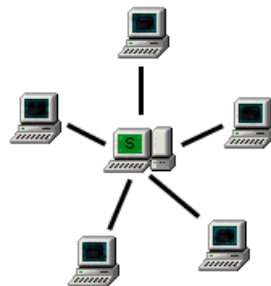   ▶ Take down material, cease conduct, publish a correction, publish an apology

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
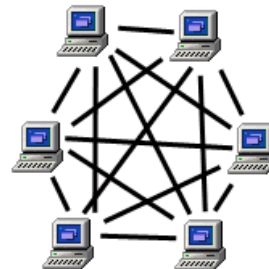
File sharing

- 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
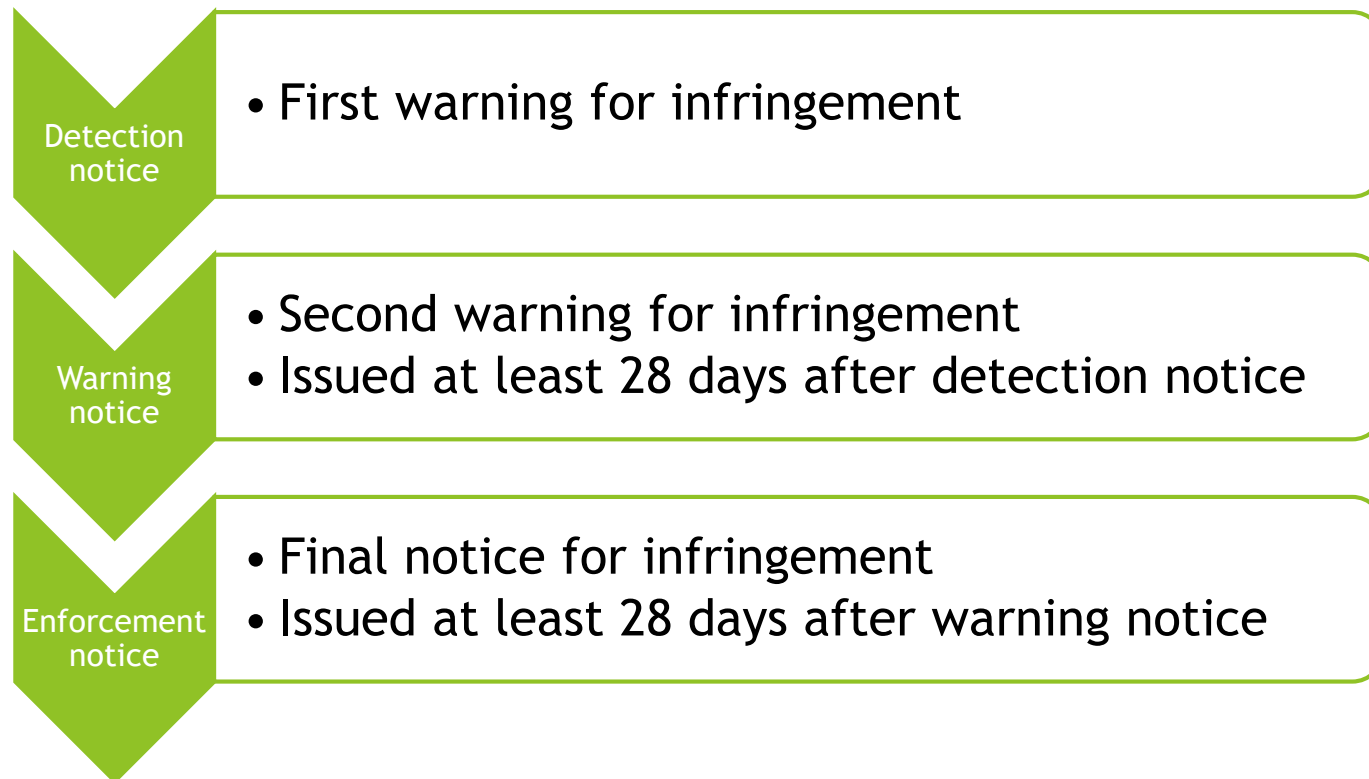
Server Based Network   Peer to Peer Network

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

- 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

Detection notice	• First warning for infringement
Warning notice	• Second warning for infringement • Issued at least 28 days after detection notice
Enforcement notice	• Final notice for infringement • Issued at least 28 days after warning 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

- Copyright Act is under review

Censorship on the Web

▶ The Office of Film and Literature Classification is responsible for determining the age classification of publications

  ▶ Includes movies, books, games, 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

▶ Web filter
  ▶ Prevents access to websites based on their content (eg. image/video screening, keywords, malware etc)

Summary

▶ Ethical issues impacting society
- ▶ Data can be used to predict and manipulate behaviour
- ▶ Online anonymity is eroding but can still be protected

▶ Ethical issues impacting individuals
- ▶ Malware includes viruses, worms, spyware, Trojan horses and logic bombs
- ▶ Online bullying and the Harmful Digital Communications Act
- ▶ Copyright Act 1994 and file sharing
- ▶ Censorship on the Web through classifications and web filtering