14. Internet Issues

14.1 The Effects of the Internet

- **Benefits:**
  - Easier access to information
  - Faster and simpler communication (individual/group)
  - Streamlined commercial transactions
  - Broad accessibility beyond privileged groups
- **Challenges:**

  Different countries have different laws for:

  - Defamation (false claims about people/organizations).
  - Pornography.
  - Political/religious comments.
  - Incitement to racial hatred.
  - Depiction of violence.

- **IT Context:**
  - Companies must comply with **cross-border laws** for hosted content
  - Social media algorithms may inadvertently promote harmful content → responsibility for IT professionals in content moderation

---

14.2 Internet Service Providers (ISPs)

- **Key Issue:** Liability for user-generated content
- **European Framework:** EC Directive 2000/31/EC → implemented in UK as Electronic Commerce Regulations 2002
  - Roles of ISPs:
    1. **Mere Conduit:** transmits data without modification, ISP not liable
    2. **Caching:** temporary storage for efficiency; ISP not liable if:
       - No modification
       - Complies with access/updating rules
       - Removes info after learning it was removed at source
    3. **Hosting:** stores customer data; ISP not liable if:
       - Customer acts independently
       - ISP unaware of unlawful activity or removes it promptly once aware
- **US Comparison:**
  - Broader ISP immunity, even for hosting
  - ISPs often **remove content to avoid risk**, potentially censoring lawful content
- **Anonymous/Pseudonymous Posts:**

    - UK: ISP can release identity if legally required
    - US: Generally cannot release unless serious crimes
- **IT Context:**
    - ISPs must implement **content management and removal workflows**
    - Systems should log complaints and removal actions for **legal compliance**

14.3 Modernising the Legislation

- **EU Digital Services Act (proposed):**
    - Transparency in advertising (targeted ads)
    - Combat disinformation and illegal content
- **UK Online Safety Bill (proposed):**
    - Duty of care for social media/search engine providers
    - Proactive detection/removal of harmful content
    - Transparency of algorithms → prevent distress/harm
    - Regulation by Ofcom
- **IT Context:**
    - IT professionals must **review content moderation, data use, advertising practices**
    - Systems need capability for **algorithm oversight, content filtering, and reporting**

14.4 The Law Across National Boundaries

14.4.1 Criminal Law

- **Extradition:**
    - Offender in Country B for crime in Country A → can be extradited if treaty exists and act is criminal in both countries
    - Some countries claim **extraterritorial jurisdiction** for serious crimes (e.g., child sexual abuse)
- **IT Context:**
    - Publishing content legal in one country may be illegal elsewhere → risk if visiting that country
    - IT operations must **consider jurisdictional differences** for website content

---

14.4.2 Convention on Cybercrime

- Covers:
    - Internet crimes (copyright infringement, hacking, fraud)
    - Child sexual abuse imagery
    - Optional: incitement to racial/religious hatred

- **IT Context:**
    - Global IT operations must comply with international agreements if participating in these regions
    - Ratification delays → uneven enforcement across countries

---

14.4.3 Civil Law

- **Contracts:**
    - Multi-country contracts should **explicitly state governing law**
- **Intellectual Property:**
    - International agreements exist, enforcement can be difficult
    - Plaintiffs often choose jurisdiction **practically** based on assets and legal efficiency
- **Example:** ISP hosting user content in multiple countries
    - Legal action may be initiated in any relevant country
    - Practical enforcement often in country with ISP presence or sympathetic law
- **IT Context:**
    - IT professionals should **design systems with clear jurisdiction and compliance tracking**
    - For international users, ensure **T&Cs and content policies reflect applicable laws**
- **Trans-Tasman Proceedings Act 2010:**
    - Simplifies cross-country disputes between NZ and Australia

14.5 Defamation

- **Definition:**
    - Making **false statements** that:
        - Damage someone's reputation
        - Bring them into contempt
        - Cause others to dislike them
    - UK distinction:
        - **Slander** → spoken
        - **Libel** → written/recorded (including emails, web pages)
- **Example Scenario:**
    - University student posts online that a referee is corrupt
    - Referee claims reputation damage → potential financial loss
    - Key issue: can the student or university be sued?
- **Key Legal Requirements (Defamation Act 2013):**
    - Claim must show **serious harm** (actual or likely financial loss)
    - Law modernized to prevent trivial claims
- **Who can be sued:**
    - **Author** of the defamatory statement
    - **Editor**
    - **Publisher**

    - Website operators (e.g., university) may **not be liable** if not responsible for posting content
- **Possible Defences (simplified):**

1. Defendant is **not the author/editor/publisher**
2. Statement is **substantially true**
3. Statement is a **clear opinion** with a basis
4. Published in the **public interest**
5. Website operator **not responsible** for posting (provided author not under operator's control)
6. Published in a **peer-reviewed scientific/academic journal**
7. Statement **protected by privilege** (e.g., court reports)

- **Website/ISP Responsibilities:**
    - Must have a **complaint handling process**
    - Respond to complaints promptly:
        - 48 hours to notify author (excluding non-working days)
        - Up to 5 days for author to respond
        - If no/insufficient response → **remove content**
    - Aim: prevent website operator from being held liable
- **International Issues:**
    - **US Law:** more favorable to authors/publishers (First Amendment)
        - Public figures must prove **malicious/reckless intent**
    - **Cross-border publication:**
        - UK resident defamed by US website → UK law may apply if ISP has **legal presence in UK**
        - US courts unlikely to enforce UK law
    - Example cases:
        - **Lalit Modi (2010):** tweeted defamatory allegation about Chris Cairns → UK court awarded £90,000 damages
        - **Justin Bieber (2020):** legal action against tweets → delayed, later dropped

14.7 SPAM

Definition

- According to the **UK Information Commissioner's Office (ICO):**

  Spam = emails sent **without your knowledge or consent**, often for marketing purposes.

- Characteristics:
    - Sent to **large numbers of recipients** without checking interest
    - Often includes **dubious content**: e.g., Viagra, penis enlargement, porn, financial scams
    - Can be **irritating, offensive**, and may carry **viruses or malware**
- **Global trend:**
    - 2014 → 70% of global email traffic was spam
    - 2021 → reduced to 43% (Statista)
- **Impacts of spam:**

- Users may be defrauded or have accounts compromised
- Important emails may be missed
- Reduces **internet effectiveness** due to unnecessary load

Technical Measures Against Spam

- Close loopholes that allow spammers to **relay through others' computers**
- **Machine learning** and algorithms to identify suspicious emails
- **Virus detection** to reject infected emails
- Maintain **stop lists** of known spam sources
- Scan **URLs** in emails for malware
- Caveats:
  - Requires **constant vigilance**
  - Risk of **false positives** → legitimate emails blocked
  - More suitable for **organizations** than individuals
  - Most email apps now include basic **spam filters**

14.7.1 European Legislation

Directive: Privacy and Electronic Communications Directive (2002/58/EC)

- Implemented in the UK via **PECR 2003** (with amendments up to 2018)
- Remains part of UK law post-Brexit

Key rules on unsolicited email:

1. Can only email **individuals** with prior **consent** (opt-in)
2. Must **provide sender's address** and a valid means to stop mailings
3. If email collected during sale of goods/services:
   - Can send direct marketing **only with easy opt-out**
4. **Definition of email:** includes text messages and social media direct messages

Consent Requirements (aligned with GDPR 2018):

- **Clear, explicit opt-in** required
- Pre-checked boxes = **not valid consent**
- Each type of communication should have **separate consent**

Enforcement:

- ICO responsible for penalties
- Max fine: **£500,000**

Weaknesses:

- Only effective for EU-origin spam
- Individuals must **take action against spammers**
- Enforcement is **time-consuming and often low-value**

Soft Opt-in Provision:

- Businesses can email **existing customers** about similar products/services
- Conditions:
    - Must market **own goods/services**
    - Only **commercial marketing** (not political/charitable)
    - Must have collected data **directly** (cannot buy lists)
    - Must provide **opt-out** option at first contact and all future communications

---

14.7.2 Legislation in the USA

Act: CAN-SPAM Act 2003 (effective 2004)

- Key difference:
    - Legal to send spam **unless recipient objects**
    - Must include **valid return address** to opt-out
- Problems:
    - Users must respond to spam → **confirming valid email**
    - Responsibility is **on recipient** (unlike EU, where it's on sender)

Other provisions:

- Illegal to **forge routing information**
- ISPs can **sue spammers**
- Examples:
    - 2005: Microsoft vs. Robert Soloway → $7.8 million judgment
    - Robert Braver (ISP) awarded $10 million
    - 2008: Soloway sentenced to 47 months + $700,000 for email fraud

---

14.7.3 Registration

Concept:

- UK & USA allow **telephone numbers to be registered** to block unsolicited calls
- This is **harder to replicate for email** because:
    - No billing records per email
    - Emails **cost same to send locally or globally**

    - Spoofing and relaying make source **hard to trace**

Limitations of email opt-out:

- PECR soft opt-in allows **direct marketing to customers** who have purchased similar products
- Cannot be used by:
    - Charities or political parties
    - Businesses using **bought-in contact lists**
- Must always allow **opt-out**

✅ Summary Points

- Spam = **unsolicited, often harmful emails**
- **Technical solutions** help but cannot fully stop spam
- EU: **PECR + GDPR** → sender must get consent
- USA: **CAN-SPAM** → recipient must object
- **Soft opt-in** allows some marketing to existing customers
- **Registration & blocking** easier for phones than email due to traceability issues

14.8 COOKIES AND USER TRACKING

Definition and Purpose

- **Cookies** = small pieces of data stored in a user's browser when visiting a website.
- **Uses:**
    - **Login/session management** (e.g., remember user authentication)
    - **Analytics** (track site usage)
    - **Personalization** (track viewed products to target ads)
- **Third-party cookies:**
    - Set by external providers
    - Track users across **different websites**
    - Used for **personalized advertising**

Regulatory Requirements

PECR (Privacy and Electronic Communications Regulations):

- Websites must **inform users** if cookies are being used
- Users must have the **option to decline** non-essential cookies
- Declining cookies may **limit functionality**, e.g., search history resets

GDPR (2018) impact:

- Cookies require **consent** as the legal basis for data processing
- Consent must be:
    - **Explicit** and **obvious**
    - **Flexible:** users can choose which types of cookies to accept
    - Not pre-checked; users must **actively opt-in**

Types of Cookies

1. **Required cookies**
    - Essential for website operation
    - No choice for users; site cannot function without them
2. **Functional cookies**
    - Maintain website functionality (e.g., forms, preferences)
    - Users may choose to decline
3. **Performance cookies**
    - Track site usage for analytics (e.g., page visits, navigation)
    - Optional; provides insights for site improvement
4. **Advertising cookies**
    - Track users across websites
    - Used for personalized ads by **third-party providers**
    - Optional; impacts site revenue if declined

Key points:

- Authentication cookies **do not require consent**
- Users can accept some cookies while declining others
- Websites often provide **detailed consent lists** for hundreds of third-party trackers
- Some dialogs combine **consent and legitimate interest**, but legal validity may vary

---

Challenges and Observations

- Users often **click "Accept All"** due to overwhelming choices
- Difficult for average users to understand scope of tracking
- GDPR penalties have motivated compliance
- Cookies are **not the only tracking method**, but remain the most common
- Legislation impacts any organization **handling EU/UK citizens' data**

14.9 CONSUMER CONTRACTS REGULATIONS (2013)

Scope:

- Governs **distance selling** (internet, phone)
- Replaced **2000 regulations**
- Still applies in the UK post-Brexit

Supplier Information Requirements (Before Contract)

Schedule 2 Requirements:

- Supplier name and address
- Description of goods/services
- Total cost including **tax**
- Delivery charges and **method of delivery**
- Method of payment
- Customer **cancellation rights** and complaint handling
- Communication costs (e.g., premium-rate calls)
- Offer validity period
- Contract duration (if not one-off)

Presentation:

- Information must be **clear and understandable**
- Can be provided **physically or digitally**
- Supplier must **fulfill contract within 30 days** unless agreed otherwise

---

Right to Cancel

- Standard cancellation period: **14 days**
    - Goods: from delivery
    - Services: from contract agreement
- Extended cancellation period: up to **12 months** if supplier failed to provide required information
- Supplier must **reimburse within 14 days** of cancellation

Exceptions:

- Customised goods
- Newspapers/magazines
- Digital downloads (e.g., movies) once download starts
- Protection against **pre-checked extras** (e.g., insurance cannot be automatically added)

Key Principles

- Ensures **consumer clarity** about purchase
- Prevents **hidden costs or unfair practices**
- Protects consumers in **online transactions** similar to offline rights
- Aligns with other online protections (cookies, email marketing, etc.)