Chapter 12: Software Contracts and Liability

Purpose of Contracts

- Contracts establish foundations for professional relationships, defining duties and responsibilities.
- They are enforceable by law and ensure collaboration between parties.

Key Terms:

- **Contract**: A legal agreement between two or more parties.
- **Breach of Contract**: Failure to perform as agreed.

Essential Elements of a Contract

- **Offer**: Promise to perform or not perform an action.
  Example: "I'll pay $500 if you rake the leaves."
- **Acceptance**: Agreement to the offer.
- **Awareness**: Both parties understand and agree to the terms.
- **Consideration**: Something of value exchanged (e.g., payment).
- **Capacity**: Legal ability to enter into a contract.
- **Legality**: Must adhere to applicable laws.

Potential Question: What are the six essential elements required for a contract to be enforceable?

Types of Software Contracts

1. **Fixed-Price Contracts:**
   - The set fee agreed upon at the start.
   - Favors clients: risks underpaying developers if scope changes.
   - Key Risk: Scope creep (e.g., adding features mid-project).
2. **Time and Materials Contracts:**
   - Costs based on time and resources.
   - Flexible but prone to disagreements over material costs.
3. **Consultancy and Contract Hire:**
   - Short-term hires to "try out" roles.
   - Useful for roles like graphic design or accounting.

Potential Question: Compare the advantages and drawbacks of fixed-price and time-and-materials contracts.

Fixed-Price Contracts:

- **Advantages**:
  - Easy to set up and favors the client, as the budget is fixed.
  - Prevents unexpected costs if the scope remains constant.
- **Drawbacks**:
  - Developers may be underpaid if the scope changes.
  - Complex projects may lead to incorrect cost estimation, causing a loss for either party.

Time-and-Materials Contracts:

- **Advantages**:
  - Flexible and accommodates changes during development.
  - Developers are paid for actual work, reducing underpayment risks.
- **Drawbacks**:
  - Prone to disputes over material costs and timelines.
  - Can result in higher costs if poorly managed.

Key Clauses in Software Contracts

1. **Project Scope**: Outlines tasks, deliverables, and timelines.
   Example: Clear deadlines help prevent scope creep.
2. **Payment Terms**: Specify method, amount, and timeline for payments.
3. **Intellectual Property (IP) Rights:**
   - Clarify software ownership post-development.
   - Developers often assume reuse rights unless clarified.
4. **Non-Disclosure Agreements (NDA):**
   - Prohibit sharing confidential project information.
   - Specify the duration of confidentiality.
5. **Non-Compete Clauses:**
   - Prevent developers from creating similar software for competitors.
   - Legally tricky and requires clear boundaries.
6. **Warranties and Liabilities:**
   - Define responsibilities and reimbursements for damages.

Potential Question: Why is an NDA critical in a software contract?

A Non-Disclosure Agreement (NDA) ensures confidentiality by:

- Prohibiting either party from disclosing sensitive project information to outsiders.
- Protecting intellectual property, trade secrets, and proprietary data.
- Holding violators liable for damages caused by information leaks.
  Example: A developer leaking confidential source code could lead to financial losses for the client.

NDAs safeguard competitive advantages and maintain trust between parties.

Software Liability and Warranty

- **Warranties**: Promises and commitments from both parties.
  - ✓ Should include expected standards of work, following laws, and fulfilling contract terms.
  - ✓ May include specific company policies to be followed by the development team.
- **Liabilities**: Situations where the development team must reimburse the client due to breaches or claims.
  - ✓ Example: If a user sues the client due to damages caused by the software, the team may not be liable unless explicitly stated
- Liability arises from defective software causing damage.
- Developers can mitigate risks with insurance (e.g., errors and omissions insurance).

Potential Question: Discuss the implications of software liability with real-world examples.(Major Software Failures Leading to Liability)

Software liability arises when defective software causes harm. Examples include:

1. Toyota Prius:
   - A software glitch caused vehicles to stall, leading to lawsuits and recalls.
   - In one case, Toyota paid $15.8 million in damages to a California car dealer.
2. Boeing 737 MAX:

- Software defects in the automated control system caused fatal crashes.
- Hundreds of lawsuits were filed, and Boeing faced significant financial and reputational losses.

3. Tesla Model S/X:
   - A touchscreen failure affecting safety systems led to a recall of 135,000 vehicles.

These cases highlight the importance of testing, insurance, and liability clauses in contracts.

Breach of Contract

1. **Types of Breach:**
   - **Actual Breach**: Failure to perform duties.
   - **Non-Payment**: Failure to pay as agreed.
   - **Misrepresentation**: Providing false information.
   - **Inadequate Performance**: Poor-quality delivery.
2. **Examples:**
   - A contractor failing to complete renovations (actual breach).
   - Late payment for goods (non-payment).

Potential Question: What remedies are available for a breach of contract?

Remedies for breach of contract include:

- **Damages**: Compensation for financial loss due to the breach.
  Example: Hiring another contractor to complete unfinished work.
- **Specific** Performance: A court order requiring the breaching party to fulfill their obligations.
- **Rescission**: Canceling the contract and returning parties to their original state.
- **Reimbursement**: Covering additional costs caused by the breach.

CONSULTANCY AND CONTRACT HIRE

Important Aspects of a Consultancy Contract

1. **Confidentiality**:
   - ✓ Consultants may have access to sensitive business information and must agree to confidentiality terms to avoid misuse.
2. **Terms of Reference:**
   - ✓ The contract should clearly define the scope of work. However, issues can arise if the consultant discovers the need to address matters outside the original scope, which the client may not want to include.
3. **Liability**:
   - ✓ Consultants may limit their liability for any losses resulting from their advice. Clients may require proof of professional liability insurance.
4. **Control Over the Final Report:**
   - ✓ The contract usually requires a draft report to be reviewed by the client, allowing for revisions before final submission.

What is Contract Hire?

- ✓ A contract hire is a short-term job that allows both the employer and the contractor to assess the fit before committing to full-time employment.
- ✓ This is also known as "temp to hire."
- ✓ After the trial period, the employer can decide whether to offer full-time employment.

Example:

1. **Hiring a Full-Stack Developer for Web Application:**
   - ✓ **Scope: Develop both the front-end and back-end of a web application.**
   - ✓ **Timeline: 12 weeks, with possible maintenance extension.**
   - ✓ **Payment: Fixed fee with milestones for each development phase.**
   - ✓ **Deliverables: A fully functional web application, documentation, and post-launch support.**

Why Do Businesses Use Contract-to-Hire Jobs?

Benefits of Contract-to-Hire:

- ✓ **Allows businesses to evaluate a candidate's performance and how well they fit within the company culture before offering full-time employment.**
- ✓ **It helps assess the importance and long-term nature of the role.**
- ✓ **Reduces hiring risks, as both parties can assess the working relationship.**

Benefits of a Cost-Plus Contract

- ✓ **Eliminates Risk:**
  - **Contractors are reimbursed for expenses, reducing the financial risk for them.**
- ✓ **Improved Quality:**
  - **Contractors can focus on the quality of work without cutting corners to save costs.**
- ✓ **Clear Communication:**
  - **Defines what each party is responsible for, reducing misunderstandings during the billing process.**

Drawbacks of a Cost-Plus Construction Contract

- ✓ **Difference of Opinions:**
  - **Disagreements can arise over what constitutes a fair cost, especially for materials. Such disputes may result in legal conflicts.**
- ✓ **Undefined Timelines:**
  - **There is often no clear incentive for contractors to finish promptly, as they are guaranteed a profit based on the time and materials used.**

This can lead to delays.

Outsourcing

- Hiring external teams for services like software development or QA.
- Options: Onshore, nearshore, offshore.
- **Points to Address in Contracts:**
  - Performance monitoring.
  - IP rights.
  - Disaster recovery plans.

EXAMPLES OF BREACH OF CONTRACT

- ✓ **Actual Breach**: Occurs when one party fails to perform as agreed (e.g., a contractor fails to complete work on time).
  - Remedies: Damages, specific performance, or contract termination.
- ✓ **Non-payment or Late Payment**: A breach occurs if a customer fails to pay as agreed (e.g., failure to pay for goods within 30 days).

- Remedies: Payment of outstanding amount, interest, damages, or termination.

- ✓ **Misrepresentation or Fraud**: Occurs when one party lies or hides crucial information (e.g., a car dealer misrepresents the condition of a car).
  - Remedies: Rescission (cancel the contract), damages, or criminal prosecution.
- ✓ **Inadequate Performance or Quality of Work**: When work does not meet agreed standards (e.g., a painter does not match the agreed color and style).

Potential Question: What are the benefits and challenges of outsourcing IT services?

Benefits:

- Cost savings, especially with offshore outsourcing.
- Access to specialized skills and technologies.
- Flexibility to scale operations based on project needs.

Challenges:

- Managing performance and ensuring quality.
- Potential legal and IP concerns if agreements are unclear.
- Communication barriers in offshore outsourcing.

Addressing these challenges with clear contracts and monitoring systems ensures successful outsourcing relationships.

Potential Question: How can contract terms ensure successful project outcomes?

Contract terms ensure success by:

- **Defining Scope**: Clearly listing tasks, deliverables, and deadlines to prevent disputes.
- **Setting Payment Terms:** Stating the payment method, timeline, and penalties for delays.
- **Establishing Ownership:** Clarifying IP rights to avoid future conflicts.
- **Incorporating Clauses**: Including NDAs, non-compete clauses, and dispute resolution mechanisms to protect both parties.
- *Example*: A graphic designer contract specifying deliverables like a logo and marketing materials ensures clarity and accountability.

****
****

Intellectual property rights

Introduction

- Property such as bicycles or computers is called **tangible property**, that is, property that can be touched. It is protected by laws relating to theft and damage.
- Property that is intangible is known as **intellectual property**. It is governed by a different set of laws, concerned with **intellectual property** rights, that is, rights to use, copy, or reveal information about intellectual property.
- **Intellectual property** crosses national borders much more quickly than tangible property and the international nature of intellectual property rights has long been recognized.

1. What is the difference between tangible and intangible property?

- **Tangible property**: Physical items like bicycles or computers, protected by laws related to theft and damage.
- **Intangible property**: Intellectual creations (e.g., ideas, software) governed by intellectual property rights laws, focusing on use, copying, or revealing information.

2. Why are intellectual property rights important on an international level?

- Intellectual property crosses national borders faster than tangible property, necessitating international laws to govern its use and protection.

Copyright

What does copyright protect?

Copyright protects:

- original literary, dramatic, musical and artistic works.
- sound recordings, films, broadcasts and cable transmissions.
- the typographical arrangement of published editions.
- Things protected by Copyright are called "works".

Software copyright

- The 1988 Copyright, Patents and Designs Act states that the phrase 'literary work" includes a table or compilation, a computer program and preparatory design material for a computer program.
- EU directive 91/250 states that “Member States shall protect computer programs, by copyright, as literary works. For the purposes of this Directive, the term ‘computer programs’ shall include their preparatory design material.”

Owner’s rights

What rights does copyright give to the owner?

Copyright gives five exclusive rights to the owner of the copyright:

- the right to copy the work.
- the right to issue copies to the public.
- the right to perform, play or show the work to the public.
- the right to broadcast the work or transmit it on a cable service.
- the right to make an adaptation of the work.

How long do the rights last?

- **In the EU**, 70 years from the death of the author (in the case of a literary or artistic work, or software).
- **In the USA**, the same is true for works published after 2002, but can be 95 years after the date of publication in some cases, for earlier works.
- **In Canada**, it is 50 years from the death of the author.

Database right (Copyright and rights in databases regulations1997)

- If a database is the author’s “own original intellectual creation”, it is treated as a literary work and it is subject to copyright protection.
- If there has been “substantial investment in obtaining, verifying or presenting the contents of the database”, then it is also protected by the database right. (**This lasts for 15 years**, much less than copyright which is much longer than the database is likely to be useful.)

Who owns the copyright?

- If the author is an employee and the work is an original literary, dramatic, musical or artistic work created in the course of employment, then the copyright belongs to the employer.
- An independent contractor is not an employee and so will own the copyright in the work he does unless agreed otherwise.
- Copyright can only be transferred in writing.
- Copyright does not need to be registered. It comes into existence at the moment the work is recorded, in writing or otherwise.

Infringement of copyright

- Anyone who, without consent, does any of the five things that are the exclusive right of the owner of the copyright has committed primary infringement of copyright.
- Secondary infringement occurs when an infringement is performed knowingly and in the course of business.
- Primary infringement is purely a civil matter. Secondary infringement can be a criminal offence.

Registering Copyright

- In Britain and Europe, full copyright protection comes into effect immediately, when the work is ‘fixed’, i.e. recorded in some form.
- In the USA, protection is very limited unless copyright has been registered with the US Copyright Office.

When is a copy a “copy”?

- Copyright is breached by copying ‘the whole or a substantial part of the work’.
- ‘Substantial’ can also mean just a key part, which could be quite small.

- Non-literal copying, e.g. using the same design to produce a similar system written in a different language.

Licensing

- A license allows (the licensee); to use a work for some or all purposes but the owner retains ownership.
- Licenses can be exclusive or non-exclusive.
- The license may be for a fixed period, or it may be in perpetuity.
- In an assignment, the copyright owner transfers some or all of the rights of ownership to someone else (the assignee).

Examples of licenses

What are the different types of licenses for software?

- **Retail software:** a license is perpetuity to use one copy of the software on a computer of your choice. Non-exclusive.
- **Professional packages:** one year license, renewable, to run the software on a server with a specified maximum number of simultaneous users. Non-exclusive.
- **Marketing agreements:** exclusive license to sell sub-licenses in a specified geographical area.

Open-source licenses / free software

How do open-source licenses differ from free software licenses?

- An **open-source license** allows the source code to be used, modified or shared, subject to certain conditions. It is not necessarily free.
- Free software can be used without payment, but the source code may not be necessarily available and modifying it may not be permitted.

Assignment

- Copyright may be assigned for a limited or unlimited period. It may be assigned for future work as well.
- Assignments must be in writing and signed by the copyright owner.

What you can do

fair dealing, copying for:

- private study or research.
- criticism or review
- reporting current events

making back-up copies

error correction.

How can copyright owners enforce their rights?

- Search and Seizure.
- Injunctions – court orders restraining people from infringing copyright.
- Claim damages.
- Claim for profits.

Large Companies who own copyright, often prevent illegal publication of copies by threatening action or suing, that a small publisher cannot afford to defend.

What is a patent, and how does it differ from copyright?

- **Patent:** A temporary, government-granted right to prevent others from exploiting an invention.
- **Copyright:** Automatic protection for literary or artistic works without registration.
- Patents require application but offer stronger protection.

Patents

- A patent is a temporary right, granted by the state, enabling an inventor to prevent other people from exploiting his invention without his permission.
- Unlike copyright, it does not come into existence automatically; the inventor must apply for the patent to be granted. However, the protection it gives is much stronger than copyright, because the grant of a patent allows the person owning it (the patentee) to prevent anyone else from exploiting the invention, even if they have discovered it for themselves.
- Patents were originally intended to encourage new inventions, and in particular to encourage the disclosure of those new inventions.
- Inventors are often hesitant to reveal the details of their invention, for fear that someone else might copy it.
- A government-granted temporary monopoly on the commercial use of their invention provides a remedy for this fear, and so acts as an incentive to disclose the details of the invention.
- After the monopoly period expires, everyone else is free to practice the invention. And because of the disclosure made by the inventor, it is very easy to do so.
- Patent holders receive exclusive rights to make, use, or sell a utility, design, or plant.
- The patentee must file a detailed description of the invention which is published by the government.
- Public disclosure provides a reservoir of technical information.
- Some companies prefer to protect their inventions called ***Trade Secrets*** by keeping private to maintain a company's competitive advantage.

Patent may only be granted if:

What are the criteria for granting a patent?

- The invention is new.
- It involves an inventive step.
- It is capable of industrial application.
- The subject matter of the invention does not fall within an excluded class.

What cannot be patented:

- A scientific theory e.g. law of physics cannot be patented.
- A mathematical method e.g. method of calculating a square root.
- A literary work, dramatic, musical or artistic work.

Parts of the patent

Typical patent includes:

- **INID Codes (Internationally agreed Numbers for the Identification):** international system that allows elements on the patent cover page to be identified in all languages.
- **Claims** - phrases that precisely define the invention and outline the boundaries of the claimed invention (prevents infringement)

Types of patents

- **Utility patents** which may be granted to anyone who invents a machine, vital process, composition of matter, article of manufacture or any useful improvement thereof.
- **Design patents** may be granted to anyone who creates a new, original design for an article of manufacture.
- **Plant patents** may also be granted to anyone who creates or discovers or reproduces any distinct and new variety of plant (Genetic Modification).

TRADEMARKS AND TRADE NAMES

- A **trademark** is a word, phrase, symbol or design, or a combination of words, phrases, symbols or designs, which identifies and distinguishes the source of the goods of one party from those of others. Examples – *Reebok*, *Mc Donald's*, *Nike*, *Levis* etc.

To register a trademark, the mark must be: -

- distinctive, and**,** not deceptive, or contrary to law or morality, and,
- It must not be identical or similar to any earlier marks for the same or similar goods.

Selecting a Mark!

- **Generic terms:** common name of the article or services to which they are applied. They are not protectable as standalone trademarks. (Examples: *computer*, *automobile*, *shuttle*.)
- **Suggestive Marks:** suggest, rather than describe the goods or services or some characteristic thereof. Consumers must use imagination or hindsight to understand the connection.
- Although suggestive marks are self-advertisers and, thus, easier to promote than arbitrary marks, they are subject to more conflict and may be afforded a narrower scope of protection.
- **Arbitrary Marks:** created from existing words but have no meaning in relation to the goods or services with which they are used. Fanciful and arbitrary marks are easier to protect but can be more expensive to promote. (Examples: *APPLE* for computers and *TIDE* for detergent).

- **Fanciful Marks:** created from words that are coined or made up and have no meaning in relation to the goods or services. (Examples: *KODAK* for film and *EXXON* for petroleum products).

Difference between Trademarks and Service mark

- The main difference between service mark and trademark is that trademark is applicable for use only to identify products or goods produced by a business. On the other hand, a service mark is used to exclusively identify a service.

How do domain names create conflicts with trademarks?

- Domain names are globally unique and allocated on a first-come, first-served basis, while trademarks are registered nationally or regionally.
- This discrepancy can lead to cybersquatting, where someone registers a trademark as a domain name to sell it at inflated prices.

Domain Names

- *ICANN* [Internet Corporation for Assigned Names and Numbers] is an internationally organized, non-profit making corporation. Its main responsibility is ensuring the 'universal resolvability' of internet addresses.
- That is, ensuring that the same domain name will always lead to the same internet location wherever it is used from and whatever the circumstances.
- In practice, *ICANN* delegates the responsibility for assigning individual domain names to other bodies, subject to strict rules.
- Domain names were originally meant to be used just as a means of simplifying the process of connecting one computer to another over the internet.
- However, because they are easy to remember, they have come to be used as a way of identifying businesses. Indeed, they are frequently used in advertising.
- Conversely, it is not surprising that companies would want to use their trademarks or their company names as their internet domain names.
- The potential for conflict between trademarks and domain names is inherent in the two systems. Trademarks are registered with public authorities on a national or regional basis.
- The owner of the trademark acquires rights over the use of the trademark in a specific country or region. Identical trademarks may be owned by different people in respect of different categories of product.
- Domain names are usually allocated by a private organization and are globally unique; they are normally allocated on a first come, first served basis.
- This means that if different companies own identical trademarks for different categories of product or for different geographical areas, only one of them can have the trademark as domain name, and that will be the one who has applied first.
- The inconsistencies between two different systems of registration have made it possible for people to register, with their own domain names, for the trademarks belonging to some other company.
- This is sometimes known as *cybersquatting*. They then offer to sell these domain names to the owner of the trademark at an inflated price.
- It is usually cheaper and quicker for the trademark owner to pay up than to pursue legal remedies, even when these are available.

How can copyright owners enforce their rights?

1. **Search and Seizure**: Locate and confiscate infringing materials.
2. **Injunctions**: Court orders to stop infringement.
3. **Claim Damages**: Recover losses caused by infringement.
4. **Claim Profits**: Seek profits made by the infringer.

****
****

DATA PROTECTION, PRIVACY & FREEDOM OF INFORMATION

Why is privacy an important issue?

- In recent years there has been a growing fear about the large amount of information about individuals held on computer files.
- In particular it was felt that an individual could easily be harmed by the existence of computerized data about him/her which may be inaccurate or misleading and which could be transferred to an unauthorized third party at high speed and very little cost.

The Data could be.

> Healthcare records > **Criminal justice** investigations & proceedings > Financial institutions & transactions

> Biological traits, such as genetic material > **Residence** and geographical records > **Ethnicity**

> Privacy breach **>** Location-based service and geolocation

What are some examples of privacy breaches related to data mining?

Data mining: "We may use information about you that we collect from other Facebook users to supplement your profile."

- Inability to voluntarily terminate accounts (previously)
- Photo recognition and face tagging 2011
- Timeline
- Psychological effects

What is the Data Protection Act 1984?

- Freedom to process data vs. privacy of individuals.
- 1984 act was repealed by the 1998 act.
- Anyone who processes personal information must comply with the eight principles.
- It provides individuals with important rights, including the right to find out what personal information is held about them.

What was the main objective of the Data Protection Act (1998)?

Main objective of Data Protection Act was designed to protect individuals from:

- the use of inaccurate personal information or information that is incomplete or irrelevant.
- the use of personal information by unauthorized persons.
- Use of personal information other than the intended purpose

Terms of the data protection Act

- **Personal data:** It's information about a living individual.
- **Data users:** are organizations or individuals who control the contents of files of personal data – i.e. who use personal data which is covered by the terms of the act.
- **A Data subject:** is an individual who is the subject of personal data.
- **Data controller:** means a person who determines why or how personal data is processed. This may be a legal person or a natural person.

Rules of Data Processing

Processing means obtaining, recording or holding the information or data or carrying out any operations on it, including:

- organization, adaptation or alteration of the information or data,
- retrieval, consultation or use of the info or data
- disclosure of the info or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

How can the Data Protection Act help us?

- It gives us the right to see our files.
- It says those who record and use personal information must be open about how the information is used.
- It must follow the 8 principles of '*good information handling.'*

What are the eight principles of the Data Protection Act (1998)?

- **Data must be processed fairly and lawfully.**
- **Processed for specific, lawful purposes.**
- **Adequate, relevant, and not excessive.**
- **Accurate and up to date.**
- **Retained only as long as necessary.**
- **Protected from unauthorized access or loss.**
- **Not transferred outside the European Economic Area without adequate protection.**
- **Processed in line with data subjects' rights.**

Main principles of the 1998 Act

Personal data must be:

First data protection principle: fairly and lawfully processed.

- Personal data shall be processed fairly and lawfully and in particular shall not be processed unless:
- at least one of the conditions in Schedule 2 is met and
- in case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Second data protection principle: processed for limited purposes.

- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Data controllers must notify the Information Commissioner of the personal data they are collecting and the purposes for which it is being collected.

Third data protection principle: adequate, relevant and not excessive

- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Many violations of this principle are due to ignorance rather than to intent to behave in a way contrary to the Act.
- Local government has a bad record of compliance with this principle, for example shops that demand to know customers' addresses when goods are not being delivered are also likely to be in breach of this principle.

Fourth data protection principle: processed in line with your rights.

- Personal data should be accurate and, where necessary, kept up to date.

Fifth data protection principle: held securely.

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- It is necessary to establish how long each item of personal data needs to be kept. Auditors will require that financial data is kept for seven years. Action in the civil courts can be initiated up to six years after the events complained of took place so that it may be prudent to hold data for this length of time.

Sixth data protection principle: measures shall be taken against unauthorized or unlawful processing of personal data & against accidental loss or damage.

- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- The 1984 Act gave data subjects the right to know whether a data controller held data relating to them, the right to see the data, and the right to have the data erased or corrected if it is inaccurate.

Seventh data protection principle: transferred to countries with adequate data protection.

- Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Eighth data protection principle: transferred to countries with adequate data protection.

- Personal data shall not be transferred to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

What does 'processed fairly and lawfully' mean in the context of personal data?

Processing must meet at least one condition from Schedule 2 (general data) and, for sensitive data, one condition from Schedule 3.

What is a common example of non-compliance with the principle of relevance?

Retailers asking for customer addresses when goods are not being delivered.

Rights of Data Subjects

What rights does the Data Protection Act provide to data subjects?

The 1998 Act extends this right of access so that data subjects have the right to receive:

- a description of the personal data being held.
- an explanation of the purpose for which it is being held and processed.
- a description of the people or organizations to which it may be disclosed.
- an intelligible statement of the specific data held about them.
- a description of the source of the data.

Data protection Act in Pakistan

The following Data Protection acts Exists in Pakistan:

- The electronic data protection and safety act 2005
- Prevention of Electronic Crimes Ordinance, 2007, 2008, 2009, 2012.
- Prevention of Electronic Crimes Act, 2014

Laws governing data privacy:

- **GDPR:** Regulates the collection and processing of personal data in the EU.
- **National data protection laws**: Countries like Canada, Japan, and Australia have their own data protection frameworks, often modeled after the GDPR.
- **CCPA** (California consumer privacy act): Provides consumers in California with rights over their personal data, including the right to opt out of data sales.
- **HIPAA**: Regulates the handling of personal healthcare information in the U.S.

What is the primary purpose of the Freedom of Information Act?

Freedom of Information

- The primary purpose of the Freedom of Information Act is to provide clear rights of access to information held by bodies in the public sector. Under the terms of the Act, any member of the public can apply for access to such information.
- The Act also provides an enforcement mechanism if the information is not made available.
- The legislation applies to Parliament, government departments, local authorities, health trusts, doctors' surgeries, universities, schools and many other organizations.

What is the Freedom of Information Ordinance (2002) in Pakistan?

Freedom of Information Ordinance 2002

- Under the Freedom of Information law, any citizen can seek any information or record from any public body, except for information categorized by law as exempt from disclosure.
- The Right to Information Act (RTI) is an Act of the Parliament of India "to provide for setting out the practical regime of right to information for citizens" and replaces the erstwhile Freedom of information Act, 2002.
- In Pakistan, KPK and Punjab assemblies have also passed RTI acts in 2013.
- **Elements of FOI:**
  - **Proactive duty:** Public bodies must publish information regarding their activities and policies.
  - **Reactive duty:** Public bodies must respond to requests for information without requiring a reason for the request, though exceptions exist for cases involving privacy, national security, or commercial interests.

What data protection acts exist in Pakistan?

- The Electronic Data Protection and Safety Act (2005).
- Prevention of Electronic Crimes Ordinances (2007-2012).
- Prevention of Electronic Crimes Act (2014).

What are the penalties for breaching the Data Protection Act?

- Civil claims for damages by affected individuals.
- Criminal charges for serious or intentional breaches.

****
****

INTERNET ISSUES

The Internet

Benefits that the internet:

- The access to all sorts of information is much easier.
- It has made communication between people much cheaper and more convenient.
- Many types of commercial transactions are simplified and faster due to the internet.
- These benefits have been made available to very many people, not just to a small and privileged group.

Disadvantages of Internet:

- Illegal or inappropriate materials
- Addiction to online social networks
- Spread of Spam or Viruses

Internet related issues:

Lack Of Creativity	Abandonment Of Family	Lack Of Face-to-Face Communication
Internet Addiction	Privacy Disrupted	Cheating
Cyber Bullying	Insomnia	Moral Corruption
Waste Of Time	Physical Inactivity	

How do laws differ regarding published content on the Internet?

Laws:

- Every country has laws governing what can be published or publicly displayed.
- Typically, such laws address/handle defamation, that is, material that makes unwelcome allegations about people or organizations.
- They may also cover other areas such as political and religious comments, incitement to racial hatred, or the depiction of violence.
- Every country has different laws.
- In some countries, publication of material criticizing the government or the established religion is effectively forbidden.
- While in others it is a right guaranteed by the constitution and vigorously defended by the courts
- The coming of the internet (and satellite television) has made these differences much more apparent and much more important than they used to be.
- Since material flows across borders so easily, it is both much likelier that material that violates publication laws will come into a country and more difficult for the country to enforce its own laws.
- The roles and responsibilities of ISPs are a central element in the way these issues are addressed.
- In Europe, the position is governed by the European Directive 2000/31/EC. In the UK this directive is implemented through the Electronic Commerce (EC Directive) Regulations 2002
- According to EC Directive, Roles that an ISP may play **mere conduit, caching, and hosting.**

What is the role of Internet Service Providers (ISPs) under the EC Directive 2000/31/EC?

ISPs can act in three roles:

- **Mere Conduit**: Only transmit data without initiating, modifying, or selecting it.
  - Not liable for damages resulting from transmissions.
- **Caching**: Temporarily store data to increase efficiency.
  - Not liable if they do not modify the data, comply with industry rules, and act swiftly to remove unlawful content when notified.
- **Hosting**: Store customer information.
  - Not liable if unaware of unlawful activities and act promptly to remove such content upon notification.

Role of mere conduit:

- ISP does no more than transmit data.
- ISP does not:
  - initiate transmissions
  - select the receivers of the transmissions.
  - select or modify the data transmitted.
- ISP can store the information temporarily, provided this is only done as part of the transmission process.
- In case an ISP is acting as a mere conduit, the regulations won't hold it liable for damages or for any other criminal sanction as a result of a transmission.

Role of caching:

Caching roles arise when:

- Information is the subject of automatic, intermediate and temporary storage.
- for the sole purpose of increasing the efficiency of the transmission of the information to other recipients of the service upon their request
- An ISP acting in the caching role is not liable for damages or for any criminal sanction as a result of a transmission, provided that it:
  - Does not modify the information.
  - Complies with conditions on access to the information.
  - Complies with any rules regarding the updating of the information, specified in a manner widely recognized and used by the industry.
  - Does not interfere with the lawful use of the technology, widely recognized and used by the industry, to obtain data on the use of information.
  - Acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of transmission has been removed from the network, or access to it has been disabled, or the court or an administrative authority has ordered such removal or disablement.

Role of hosting:

- Where an ISP stores customer information, it is acting in a hosting role.
- In this case ISP is not liable for damage or criminal sanctions provided that:
  - It did not know that anything unlawful was going on.
  - Where a claim for damages is made, the ISP did not know anything that would lead to something unlawful.
  - When it found out that that something unlawful was going on, it immediately tried to remove the info or prevented access to it.
  - The customer was not acting under the authority or the control of the service provider.

Internet Service Providers:

How does the UK differ from the USA in ISP information release?

- In the UK, the ISP is allowed to release the information and can be compelled to do so by a court.
- In the USA, ISPs cannot in general be required to release the information, although they may be required to do so in the case of serious crimes.

Law across National Boundaries

How does criminal law apply to online content across national boundaries?

Criminal Law:

- Suppose that you live in country A and on your website, you publish material that is perfectly legal & acceptable in country A, but it is a criminal offence to publish in country B. In that case you can't be prosecuted in country A, and it is very unlikely that you would be handed over to country B. To avoid getting into trouble, you might, however, be careful in not visiting country B voluntarily.

Civil Law:

- For some parts of the civil law where the position is reasonably clear cut. Any contract that involves parties from more than one

country should, and usually will, state explicitly under which jurisdiction (that is, which country's laws) it is to be interpreted.

- Where **intellectual property law** is concerned, there are international agreements to which most countries are signatories so that there is a common framework, though it can be very difficult to enforce the rights in certain countries.

What is defamation, and how is it categorized?

Defamation:

- Defamation means making statements that will damage someone's reputation, bring them into contempt, and make them disliked, and so on.
- In British law, spoken offence is called **slander** and written is called **libel** (It could be email).
- Defendant needs to prove that:
  - He was not the author, editor or publisher of the statement complained of.
  - He took reasonable care in relation to its publication.
  - He did not know and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.
- If any objectionable material is published on, for example, newspaper, website etc. the complainant can take action against the publisher of the newspaper, and the editor etc.
- What if something objectionable is posted on a forum of a university?
  - When the libel is published on a web page, on the university site, the university can reasonably argue that it cannot possibly vet everything that every one of its 1,000 students puts on their personal web page.
  - It is not, in fact, publishing the pages, it is only providing an infrastructure that allows students to publish their own web pages. In the terminology used in the 2002 Regulations it is acting in a hosting role.
  - Provided, therefore, that it removed the offending material as soon as it had reason to suspect its presence and that the student was not acting under its authority or control, the university cannot be subject to an action for damages.
- The First Amendment to the **United States Constitution** guarantees a right to free speech that the US courts have always been eager to defend.
- The result is that many statements that might be considered defamatory in the UK would be protected as an exercise of the right of free speech in the USA.

CASE STUDY # 01

- Geneva and her friends were celebrating her 30th birthday. After a few too many glasses of champagne, Geneva climbed on a monument in the town center and sang a few verses of *Happy Birthday* to herself. A crowd gathered, and several photojournalists got some pretty incriminating shots. The next day, she saw several social media sites posted her untouched-up photos online. Angered, she cried defamation and initiated a lawsuit. What will likely happen?

Likely Outcome:

- **Defamation Claim Unlikely to Succeed:**
  - Defamation requires false statements causing harm to reputation. Untouched photos showing factual events don't meet this criterion.
- **Public Behavior is Not Private:**
  - Geneva was in a public space, reducing her expectation of privacy. Photos taken in public are typically lawful.
- **No Right to Control Public Perception:**
  - The law does not protect against embarrassment from truthful representation of public actions.
- **Possible Exceptions:**
  - If the photos were altered to misrepresent her actions, she might have grounds for a lawsuit.

Conclusion: The lawsuit will likely fail as the photos truthfully depict her public actions, and defamation does not apply.

CASE STUDY # 02

- Mrs. Crump is a Professor of English at Smartsville University. The students say she is a mean person. The administration at school loves how she pushes the students to do their best. A few students tell the college president that Crump hit them with a ruler. Then they posted signs all over campus about her alleged abuse. They even used photo-enhancing software to manipulate photos of Crump hitting students. As a result of their accusations, Crump was suspended without pay until an investigation is complete. What can Ms. Crump do?

Mrs. Crump's Alleged Abuse

- **Defamation Lawsuit:**
  - Mrs. Crump can sue the students for defamation since the accusations (hitting students with a ruler) are false, damaging her reputation, and led to her suspension.
  - Manipulated photos strengthen her claim by proving malice or intentional harm.
- **School Investigation:**
  - Cooperate fully with the investigation to clear her name and provide evidence disproving the accusations.
- **Seek Damages:**
  - If cleared, she can pursue compensation for lost wages, emotional distress, and reputational harm caused by the false accusations.
- **Potential Disciplinary Action:**
  - Request the administration take action against the students for their malicious behavior, such as suspension or expulsion.

Conclusion : Mrs. Crump can pursue legal action for defamation and seek damages

CASE STUDY # 03

- Joseph's Seafood Market was preparing for their annual Whale of a Sale on Seafood. The local food critics got the news, and one well-intended writer posted an article stating "Joseph's sells whale filets." What he meant to write was, "Joseph's is having a whale of a sale on filets." People in the community got wind of this and boycotted the store. What can Joseph do?

Joseph's Whale Filets Rumor

1. **Defamation Lawsuit:**
   a. Joseph can sue the writer for defamation since the false statement ("Joseph's sells whale filets") harmed the business's reputation and caused financial loss.
2. **Public Clarification:**
   a. Issue an immediate press release and social media posts clarifying the mistake and emphasizing that the business does not sell whale meat.
3. **Writer's Responsibility:**
   a. Request the writer publish a correction and apology prominently to mitigate the harm caused by the error.
4. **Rebuild Reputation:**
   a. Offer promotions or community engagement events to rebuild trust and attract customers back to the store.
5. **Legal and PR Balance:**
   a. Use legal action only if necessary, focusing on restoring the brand's reputation through transparent communication.

Conclusion : Joseph can clarify the mistake publicly and consider legal action if needed to restore his business's reputation.

What are the defenses against a defamation claim?

The defendant must prove:

- ✓ They were not the author, editor, or publisher of the statement.
- ✓ They took reasonable care in its publication.
- ✓ They had no reason to believe it was defamatory.

Organization for Cybercrime:
Council of Europe approved a draft convention on 'cybercrime':

- It deals with objectionable material on the internet, criminal copyright infringement, computer-related fraud and hacking.
- There is an additional protocol relating to incitement to religious or racial hatred, to which signatories to the protocol may also sign up.

Internet Watch Foundation:

What is the role of the Internet Watch Foundation (IWF)?

- In the UK, the Internet Watch Foundation (IWF) was set up in 1996 to monitor and, where desirable and possible, take action against illegal and offensive content on the UK internet.
- It has the support of the UK government, the police and the ISPs.

The Internet Content Rating Association:

- The Internet Content Rating Association (ICRA) is an international, independent organization whose mission is to help parents to protect their children from potentially harmful material on the internet, whilst respecting the content providers' freedom of expression.

Spam:

How is spam regulated in the UK and USA?

- ✓ UK: Unsolicited emails are illegal unless the recipient has given prior consent.
- ✓ USA: Legal unless the sender is informed not to send more emails or does not provide an opt-out mechanism.

Why is spam challenging to stop?

- ✓ Spammers forge sender addresses and use other mail servers.
- ✓ No reliable system exists to trace or block all spam effectively.

What are schemes to prevent unsolicited calls and spam?

- ✓ Phone calls: Registration schemes in the UK and USA allow individuals to block marketing calls.
- ✓ Spam: The CAN-SPAM Act in the USA mandates opt-out options for recipients.

What is the Council of Europe's Convention on Cybercrime?

- ✓ Addresses objectionable internet material, criminal copyright infringement, fraud, and hacking.
- ✓ Includes an additional protocol against incitement to religious or racial hatred.

- Unsolicited email sent without the consent of the addressee and without any attempt at targeting recipients who are likely to be interested in its contents.
- In the UK, the directive was implemented by the Privacy and Electronic Communications (EC Directive) Regulations 2003.
- Unsolicited email can only be sent to individuals (as opposed to companies) if they have previously given their consent.
- Sending unsolicited email that conceals the address of the sender or does not provide a valid address to which the recipient can send a request for such mailings to cease is unlawful.
- In the USA it is the responsibility of the recipient to inform the spammer that he doesn't want to receive the spam. It is legal to send spam if:
  - The person sending the spam has not been informed by the receiver that they do not wish to receive spam from that source.
  - The spam contains an address that the receiver can use to ask that no more spam be sent.
- Registration of Phone numbers:
  - Both the USA and the UK operate successful schemes that allow individuals to register their phone numbers as ones to which unsolicited direct marketing calls must not be made.
  - This should act as a model for preventing spam; indeed, the CAN SPAM Act specifically requires the Federal Trade Commission to produce plans for such a register within six months.
  - Unfortunately, the technical differences between the internet and the telephone network make this model unlikely to work with spam.
- Spamming is easy due to forging the sender's address on an email, and also using other people's mail servers to send you mail. Due to this fact there are no reliable records that can be used to identify where the spam really came from or to stop it completely.

In most cases, use of the internet is not charged on the basis of individual communications but on the basis of connect time, so there is no recording of individual emails and it costs the same to send an email from Australia to the UK than it does to send an email to one's colleague in the next office.

COMPUTER MISUSE

Background

- In recent years, the public has been much more concerned about the misuse of the internet than about the more general misuse of computers.
- Nevertheless, crimes committed using computers form a significant proportion of so-called **white-collar crime** and it has been necessary to introduce legislation specifically aimed at such activities.

What is cybercrime, and how is it defined legally?

Cyber Crime

- An act against the public good
- Each statute/Law that defines a crime must specifically explain the conduct that is forbidden by that statute.
- No act can be considered a crime unless it is prohibited by the law of the place where it is committed and unless the law provides for the punishment of offenders.

What are computer crimes? Provide examples.

Computer Crime

- Computer crimes refer to the use of information technology for illegal purposes or for unauthorized access to a computer system where the intent is to damage, delete or alter the data present in the computer. Even identity thefts, misusing devices or electronic frauds are considered to be computer crimes.

The Misuse of Computers Act 1990

What are the categories of computer misuse under the Act?

Categories of Misuse:

- computer fraud.
- unauthorized obtaining of information from a computer.
- unauthorized alteration or destruction of information stored on a computer.
- denying access to an authorized user.
- unauthorized removal of information stored on a computer.

Computer Fraud

What is computer fraud, and what are its categories?

Computer Fraud categories:

- Input fraud > Output fraud > Program fraud (salami-slicing)

The Law Commission defined computer fraud as:

- conduct that involves the manipulation of a computer, by whatever method, dishonestly obtain money, property, or some other advantage of value, or to cause loss.

The main offences currently covering computer fraud:

> fraud and theft; > obtaining property by deception; > false accounting.

Unauthorized Obtaining of Information

The Law Commission identified three particular abuses:
> computer hacking; >eavesdropping on a computer; >making unauthorized use of computers for personal benefit.
Historically, it has been difficult to convict anyone of computer hacking.

What is the purpose of Section 1 and Section 3 of the Computer Misuse Act?

- ✓ **Section 1:** Deterring unauthorized access (hacking).
- ✓ **Section 3**: Criminalizes unauthorized modification of data or programs, impairing operations, or hindering access.

Under Section 1 of the Computer Misuse Act 1990, a person is guilty of an offence if:

- He causes a computer to perform any function with intent to secure access to any program or data held on any computer.
- the access he intends to secure is unauthorized.
- He knows at the time when he causes the computer to perform the function that this is the case.
- This offense is punishable by up to a **£5,000 fine** or **six months' imprisonment**

SECTION 1: THE MAIN PURPOSE OF THIS SECTION IS TO DETER HACKERS!
SECTION 2: Unauthorized Access with Intent to Commit a Serious Crime

Eavesdropping involves:

– secret listening; – secret watching.

- The aim is the acquisition of information.
- Historically, there has been no right to privacy in the UK.
- The recently introduced UK Human Rights Bill incorporates the European Convention on Human Rights into UK law.
- Privacy is now recognized as a basic human right. For instance, listening to mobile telephone calls is now illegal.
- Most people who misuse computers for personal benefit are in some form of legal relationship with the owner of the computer.
- For example, an employee who does private work on their employer's computer.
- Here **employment law** can be applied. The unauthorized use of the computer is not a special issue.
- This offense carries a penalty of up to **five years' imprisonment** or an **unlimited fine**.

Unauthorized Altering or destruction of Information

Computers store vast amounts of information about us:

>what we have in the bank; > who we call on the telephone;> what we buy in the shops; >where we travel.

Criminals who **alter or destroy** such information can be dealt with by

>the law on Criminal Damage; **>** the Computer Misuse Act 1990 section 3

The law on Criminal Damage seems to apply to physically stored data for example:

> Damage or Delete data belonging to someone **>** writing a program that damages the data on a hard disk.

But not:

>switching off a monitor so that the display can't be seen.

Unauthorized Modification

Section 3 of the Computer Misuse Act 1990 provides that a person is guilty of a criminal offence if:

- he does any act which causes unauthorized modification of the contents of a computer.
- At the time when he does the act, he has the requisite intent and the requisite knowledge.

The requisite intent is an intent to cause a modification to the contents of any computer and by doing so:

- to impair the operation of any computer.
- to prevent or hinder access to any program.
- to impair the operation of any such program or the reliability of any such data.

What is the requisite intent for unauthorized modification under the Act?

The intent must include:

- ✓ Modifying data to impair operations of a computer or program.
- ✓ Hindering access to data or programs.
- ✓ Compromising data reliability.

Forgery

The unauthorized alteration or destruction of data may amount to forgery.

The Forgery and Counterfeiting Act 1981 says:

- A person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it, to do or not to do some act to his own or any other person's detriment.

An "instrument" is usually a written document. However, it can also be "any disk, tape, soundtrack or other device on which information is stored by mechanical, electronic or other means."

E.g., A forged electronic mail message

Denying Access to an Authorized User

There are many ways to deny access to an authorized user of a computer:

- shut the machine down.
- overload the machine with work.
- tie up all the machine's terminal/network connections.
- encrypt some system files…. etc.

Various offences deal with:

- hacking.
- unauthorized obstruction of electricity.
- improper use of telecommunications services.
- unauthorized modification of computer material.

Unauthorized removal of Info. stored on a computer.

- Under the Theft Act 1968, only property can be stolen, and information is not property.
- A floppy disk is protected by law, but the information stored on it is not.

Examples 1

- A student hacks into a college database to impress his friends - **unauthorized access.**
- Later he decides to go in again, to alter his grades, but cannot find the correct file - **unauthorized access with intent**...
- A week later he succeeds and alters his grades - **unauthorized modification of data.**

Examples 2

- An employee who is about to be made redundant finds the Managing Director's password; logs into the computer system using this and looks at some confidential files- **unauthorized access.**
- Having received his redundancy notice he goes back in to try and cause some damage but fails to do so - **unauthorized access with intent...**
- After asking a friend, he finds out how to delete files and wipes the main customer database - **unauthorized modification.**

Reasons for Cyber Crime not being reported.

It is tough to punish a Cyber-crime criminal because:

- Offences are difficult to prove.
- Evidence is difficult to collect - firms usually do not cooperate with the police.
- Firms are embarrassed or scared about their reputation due to hacking - particularly banks.
- Employees are normally sacked or demoted.
- Police lack expertise, time, money.
- Cyber-Crime is perceived as 'soft crime', as no one gets physically injured or hurt.

Current situation

- Hacking has increased with time, both as a prank and as a professional crime.
- A few high-profile cases are reported in the past.
- **Offenders are often in other countries with no equivalent legislation.**
- Some 'international task forces' set up but no real progress.

Pakistan Cyber Crime Bill-2016

- Electronic Transaction Ordinance 2002
- Electronic / Cyber Crime bill 2007

Electronic Transaction Ordinance 2002

■ Overview

- The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation created by national lawmakers.
- A first step and a solid foundation for legal sanctity and protection for Pakistani E-Commerce locally and globally.
- Laid the foundation for comprehensive Legal Infrastructure.
- It is heavily taken from foreign law related to cybercrime.

Electronic/ Cyber Crime Bill 2007

What is electronic forgery, and what is the punishment under the Cybercrime Bill (2007)?

Overview

- "Prevention of Electronic Crimes Ordinance, 2007" is in force now.
- It was promulgated by the President of Pakistan on the 31st of December 2007
- The bill deals with the electronic crimes included:

  > Cyber terrorism > Data damage > electronic fraud

  > electronic forgery > Unauthorized access to code

  > Cyber stalking > Cyber Spamming

Sections

Data Damage

- Whoever with intent to illegal gain or cause harm to the public or any person, damages any data, shall come under this section.

Punishment

- 3 years
- 3 lacs

Electronic Fraud

- People for illegal gain get in the way use any data, electronic system or device or with intent to deceive any person, which act, or omission is likely to cause damage or harm.

Punishment

- 7 years

- 7 lacs

Electronic Forgery

- Whoever for unlawful gain interferes with data, electronic system or device, with intent to cause harm or to commit fraud by any input, alteration, or suppression of data, resulting in unauthentic data that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not.

Punishment

- 7 years
- 7 lacs

Spamming

- Whoever transmits harmful, fraudulent, misleading,
- illegal or unsolicited electronic messages in bulk to any person
- without the express permission of the recipient,
- involves in falsified online user account registration.
- falsified domain name registration for commercial purpose commits the offence of spamming.

Punishment

- 6 Months
- 50,000

END OF CHAPTERS

8. What are examples of denying access to authorized users?
Answer:

1. Shutting down the machine.
2. Overloading the machine with work.
3. Encrypting system files.
4. Blocking terminal or network connections.

Unauthorized Access and Data Modification
9. What are the three abuses identified under unauthorized obtaining of information?
Answer:

1. Computer hacking.
2. Eavesdropping on computer systems.
3. Unauthorized use of computers for personal benefit.

10. What laws address unauthorized data modification?
Answer:

- **Criminal Damage Act**: Covers physical destruction or damage to data.
- **Computer Misuse Act (1990), Section 3**: Covers unauthorized digital modifications.

Hacking and Eavesdropping
11. What constitutes hacking under the Computer Misuse Act (1990)?
Answer:

- Accessing a computer or data without authorization, with intent to secure or modify information.

12. What is eavesdropping in a computing context, and how is it addressed legally?
Answer:

- Secretly listening or watching to acquire information.
- Privacy is protected under the UK Human Rights Bill and European Convention on Human Rights.

Cybercrime Bill 2007
13. What electronic crimes are addressed by the Cybercrime Bill (2007)?
Answer:

1. Cyber terrorism.
2. Data damage.
3. Electronic fraud and forgery.
4. Unauthorized access.
5. Cyber stalking and spamming.

14. What is the punishment for electronic fraud under the Cybercrime Bill?
Answer:

- **Punishment**: 7 years imprisonment and/or a fine of 7 lacs.

15. What are the penalties for spamming under the Cybercrime Bill?
Answer:

- **Punishment**: 6 months imprisonment and/or a fine of 50,000.

Examples of Computer Misuse

16. Provide examples of computer misuse and their corresponding offenses.
Answer:

1. A student hacking into a database to impress friends → Unauthorized access.
2. Altering grades in a database → Unauthorized modification.
3. Employee using a manager's password to view confidential files → Unauthorized access.

Challenges in Addressing Cybercrime
17. Why is cybercrime often underreported or unpunished?
Answer:

- ✓ Difficulty in proving offenses and collecting evidence.
- ✓ Companies fear reputational damage, especially banks.
- ✓ Lack of expertise, time, and money in law enforcement.
- ✓ Offenders may reside in countries with no equivalent legislation.

18. How has hacking evolved, and what is the current situation?
Answer:

- Hacking has increased as both a prank and a professional crime.
- Offenders often operate from countries with no applicable laws, making prosecution difficult.
- International task forces exist but have limited progress.

Question from Assignments and Case Studies etc:

Do you think the re-production of someone's idea is professionally and ethically allowed or not? Briefly argue on it in bullets in support and against of it.

- **Against the Reproduction of Ideas:**
  - ✓ Intellectual Property Violation: Reproducing someone else's idea without permission is a violation of intellectual property rights, such as patents, copyrights, or trade secrets.
  - ✓ Unfair Competition: Reproducing someone else's idea undermines fair competition and leads to an unethical business environment.
  - ✓ Loss of Innovation Incentives: Allowing such reproduction would discourage innovation and discourage entrepreneurs from investing in new ideas.
- **In Support of Reproduction:**
  - ✓ Public Domain: If an idea is not patented or protected, it may be open for others to reproduce and build upon.
  - ✓ Ethical Creativity: In some cases, reproducing an idea could lead to the development of a better or more accessible version of the product, contributing positively to market innovation.

Question: How to securing intellectual property and protecting business ideas from theft or unauthorized use.

- ✓ Patenting: Zainab should patent her recipe/formula to ensure that her idea is legally protected from duplication by others.
- ✓ Non-Disclosure Agreements (NDAs): She should require all employees, contractors, and business partners to sign NDAs to protect sensitive business information.
- ✓ Copyrights: If applicable, Zainab should copyright any marketing materials, branding, or product-related documentation.
- ✓ Trade Secrets: Zainab could register her formula as a trade secret and implement access control measures within her organization to ensure only authorized individuals can access sensitive data.

Question : **what clauses you would add in the contract to avoid the breach of idea**

Clauses that Zainab should include in an **Employer Contract** to avoid a breach of her idea/formula:

1. **Confidentiality Clause**: All employees should be required to keep company information confidential and not disclose it to any third party.
2. **Non-Compete Clause**: Prevents employees from starting or joining competing businesses for a specified period after leaving the company.
3. **Non-Disclosure Agreement (NDA)**: Employees should agree to keep all proprietary information, including the energy drink formula, confidential.
4. **Intellectual Property Ownership**: Clearly states that any inventions, formulas, or ideas developed during employment belong to the company.
5. **Return of Property Clause**: Requires employees to return any physical or digital company property upon resignation or termination.

6. **Penalty Clause for Breach**: Specifies penalties or consequences for violating confidentiality or IP clauses.

Question : **terms to include in a Memorandum of Understanding (MoU)** when formalizing a business partnership.

Core points to include in an **MoU** for an investor deal:

1. **Ownership and Equity Split**: Clarifies the percentage of ownership between the parties.
2. **Role and Responsibilities**: Defines the roles, responsibilities, and authority of each party in the business.
3. **Intellectual Property Ownership**: Specifies who owns the product formula, trademarks, patents, and any IP created.
4. **Investment Terms**: Details the amount of investment and the terms regarding how funds will be used.
5. **Profit Sharing**: Outlines how profits will be divided between the investor and Zainab.
6. **Exit Strategy**: Discusses terms regarding exit, dissolution, or sale of the business.
7. **Confidentiality**: Ensures both parties agree to keep business plans and proprietary information confidential.

Question : This question focuses on **international protection of intellectual property**, particularly when moving a business across borders.

- **No Automatic Protection**: If Zainab patented her formula in Pakistan, it will not automatically be protected in the USA.
- **International Patents**: She would need to apply for a **separate patent** in the USA through the U.S. Patent and Trademark Office (USPTO) or use the **Patent Cooperation Treaty (PCT)** to seek protection in multiple countries.
- **Jurisdiction-Specific Laws**: Patents are jurisdiction-specific, meaning each country has its own laws and processes for granting and enforcing patents.

Question : This question focuses on the **violation of data protection laws** and the legal consequences for breach.

- ✓ **Violation of Data Protection**: Mr. Ahmed violated **data protection laws** by accessing and stealing sensitive business data, including the recipe and customer records, without authorization.
- ✓ **Pursuing Legal Action**: Zainab can pursue Mr. Ahmed in court for **breach of confidentiality**, **theft of trade secrets**, and **data protection violations** under applicable laws. She can file a **civil suit** for damages and may also pursue **criminal charges** depending on the severity of the breach.

Question : This question refers to **contract clauses** that address penalties or non-solicitation agreements in business contracts.

Non-Solicitation Clause for Ensighten and GMI:

- **Ensighten's Interest**: Ensighten may want to prevent GMI from hiring its employees or soliciting its clients to ensure that its workforce and business relationships remain intact.
- **GMI's Interest**: GMI may want to ensure that its own workforce is not poached by Ensighten and that they can continue to operate without interference.

Q3: Steve hosts a blog site and has wrong allegations on himself for defaming a fortune 50 company on the blog site he hosts. **Guide him how he can defend himself and prove his innocence.**

Steve can defend himself against the defamation allegations by using the following legal defenses:

- ➢ Truth: Prove that the statements made on his blog are true. Truth is a complete defense to defamation.
- ➢ Opinion: If the statements are considered opinions rather than factual claims, Steve can argue that they fall under free speech protection.
- ➢ Fair Comment: Steve can argue that his blog post is a fair comment on a matter of public interest, provided it is based on facts and not malicious.
- ➢ Lack of Malice: If Steve did not intend to harm the reputation of the Fortune 50 company and the statements were made without malice, this could be a defense, especially if the company is a public figure.
- ➢ Retraction: If Steve made an error, issuing a public retraction and apology may help reduce the damage and mitigate the legal consequences.
- ➢ No Defamation: Demonstrate that the statements made were not defamatory, meaning they did not harm the reputation of the company or that they did not meet the legal definition of defamation.

Question(Software Contracts and Liability):

A government agency hired a software company for a fixed-price surveillance system contract. Midway, the agency expanded the scope to include real-time analytics, leading to a dispute over additional payment and delays. How can the contract clauses resolve this, and what negotiation strategy should both parties adopt?

Answer:

Contract Clauses for Resolution:

- **Deliverables:**
  - ➢ Review if real-time analytics falls within the originally agreed scope.
  - ➢ If undefined, consider it a new requirement outside the contract.
- **Payment Terms:**
  - Fixed-price contracts often include a **change order clause** for unforeseen changes.
  - Example: Defense contracts with cost renegotiation mechanisms, like Boeing.
- **Handling Changes:**
  - If changes are significant, the clause can formalize discussions for additional payments, timelines, and deliverables.

Negotiation Strategy:

1. **Collaborative Review:**
   - Jointly revisit the contract to confirm whether the additional requirement aligns with the original scope.
2. **Mutual Agreement:**
   - The government agency compensates the software company for extra work.
   - The company commits to revised, realistic timelines.
3. **Neutral Mediation:**
   - Engage a third party to mediate disputes and ensure impartiality.
   - Example: Tesla's collaboration with Panasonic to fund new features.
4. **Flexibility and Shared Goals:**
   - Focus on achieving project goals without escalating liabilities or delays.
   - Negotiate a win-win solution to maintain partnership and project success.

Question (Intellectual Property Rights):

A startup faces patent conflicts over its autonomous drone algorithm, with a competitor holding a similar patent. Additionally, some team members leaked source code online. How can the startup address the patent conflict and protect its intellectual property?

Answer:

Addressing the Patent Conflict:

1. **Conduct a Prior Art Search:**
   - Investigate whether the competitor's patent overlaps with publicly known concepts or lacks novelty.
   - File for **patent invalidation** if overlaps are found.
2. **File Defensive Patents:**
   - Secure patents for unique features of the startup's algorithm to strengthen its IP position.
3. **Collaborate or Negotiate:**
   - Explore cross-licensing agreements or partnerships with the competitor to avoid litigation and gain mutual benefits.
4. **Legal Action:**
   - If infringement is suspected, consider filing a lawsuit to protect the startup's IP.

Protecting Source Code:

1. **Copyright Registration:**
   - Register the software code under copyright laws to establish legal ownership and pursue infringement cases.
2. **Enforce Confidentiality Agreements:**
   - Take legal action against team members who breached non-disclosure or confidentiality clauses.
   - Example: Google sued employees for leaking AI code snippets.
3. **Strengthen Internal Policies:**
   - Restrict access to sensitive code using role-based permissions and secure repositories.
   - Use code obfuscation tools to make leaked snippets harder to understand or reuse.
4. **Employee Training:**
   - Conduct workshops on the ethical and legal implications of IP leaks.
5. **Future Deterrence:**

- Update contracts to include stricter penalties for IP breaches.
- Monitor access logs and usage of sensitive code to prevent leaks proactively.

By taking these actions, the startup can mitigate risks, protect its innovations, and maintain a competitive edge.

Question (Data Protection, Privacy):
A healthcare organization accidentally exposed sensitive patient records due to a misconfigured database and received a FOIA request about its data protection practices. How should it handle the data breach, respond to the FOIA request, and comply with privacy laws?
Answer:
Addressing the Data Breach:

1. **Immediate Actions:**
   - Notify affected individuals promptly as required by laws like **HIPAA** or **GDPR**.
   - Inform relevant regulatory authorities within mandated timelines.
2. **Forensic Investigation:**
   - Determine the cause of the database misconfiguration.
   - Document findings and implement corrective measures to prevent recurrence.
3. **Rebuild Trust:**
   - Communicate transparently with stakeholders about the breach and measures taken to enhance security.
   - Example: Anthem strengthened its systems and openly shared updates after its 2015 data breach.

Responding to the FOIA Request:

1. **Transparency Without Breach of Privacy:**
   - Provide an overview of data protection practices while redacting any sensitive or identifying patient information.
   - Cite exemptions under FOIA that protect personal privacy, if applicable.
2. **Collaborate with Legal Counsel:**
   - Ensure compliance with FOIA requirements while safeguarding patient confidentiality and proprietary practices.
3. **Detail Improvement Plans:**
   - Highlight steps taken to strengthen data protection to demonstrate accountability and commitment.

Ensuring Compliance and Future Prevention:

1. **Regular Security Audits:**
   - Conduct periodic reviews of systems to identify and fix vulnerabilities.
2. **Database Configuration Management:**
   - Implement strict access controls and automated monitoring tools for real-time error detection.
3. **Employee Training:**
   - Educate staff on privacy laws, security best practices, and proper database management.
4. **Crisis Management Plans:**
   - Establish a robust incident response plan to handle breaches efficiently and reduce impact.

By addressing the breach transparently, complying with FOIA responsibly, and enhancing data security measures, the organization can protect patient privacy while rebuilding trust and meeting legal obligations.

Question (Internet Issues):
A social media platform is sued for defamation due to user-generated content accusing a public figure of corruption. The platform claims immunity as a "mere conduit," but the plaintiff argues it actively promotes controversial posts. How does current law address this, and what reforms could clarify liability?
Answer:
Evaluation of Platform's Liability:

1. **"Mere Conduit" vs. Active Hosting:**
   - Platforms acting as "mere conduits" (e.g., passive hosts of user content) are typically immune under laws like **Section 230 of the Communications Decency Act (CDA)** in the U.S.
   - Actively promoting content (e.g., using algorithms to boost engagement) may render the platform an **active publisher**, exposing it to defamation claims.
2. **Editorial Control and Liability:**
   - If the platform exerts editorial control by amplifying specific posts, it transitions into a role similar to a publisher, which can weaken its immunity.
   - Precedents: Cases involving **Facebook** and **Twitter** have explored the limits of immunity for actively managed content.
3. **Global Perspectives:**
   - In the EU, the **Digital Services Act** imposes stricter obligations on platforms to moderate harmful content, potentially influencing similar disputes.

Potential Legal Reforms:

1. **Algorithm Transparency:**
   - Require platforms to disclose how their algorithms prioritize or amplify content, especially controversial or defamatory posts.
   - Enable clearer determination of liability based on algorithmic influence.
2. **Conditional Immunity:**
   - Modify laws like Section 230 to grant immunity only if platforms meet specific obligations, such as robust moderation practices or transparency in content promotion.
3. **Defamation-Specific Safeguards:**
   - Introduce provisions holding platforms accountable for failing to act on flagged defamatory content within reasonable timeframes.
4. **Balanced Regulation:**
   - Ensure reforms preserve **free speech** by not penalizing platforms for hosting general user-generated content, focusing instead on active amplification or negligence.

Ethical and Practical Implications:

1. **Balancing Free Speech and Accountability:**
   - Over-regulation risks stifling open discourse, while under-regulation may allow unchecked harm to reputations.
   - Example: The **Cambridge Analytica scandal** underscored the impact of opaque platform practices on public discourse and accountability.
2. **Empowering Users:**
   - Provide users with tools to understand and control how their content is promoted, fostering accountability for both creators and platforms.

By distinguishing passive hosting from active content management and implementing reforms to increase transparency and accountability, these disputes can be addressed effectively while preserving freedom of expression.

Question (Computer Misuse):
A global retail company faces a ransomware attack due to a phishing link clicked by an employee. The attackers demand payment in cryptocurrency. Should the company negotiate or refuse payment? What post-incident measures should it take to comply with the Computer Misuse Act and prevent future attacks?
Answer:
Ethical, Legal, and Practical Considerations:

1. **Negotiating with Attackers:**
   - **Ethical:** Paying the ransom may encourage further criminal activities and harm other potential targets.
   - **Legal:** Ensure compliance with anti-terrorism laws and sanctions to avoid aiding prohibited entities.
   - **Practical:** Payment might not guarantee full data recovery or prevent attackers from leaking or reselling data.
2. **Refusing Payment:**
   - **Ethical:** Avoids rewarding criminal behavior.
   - **Legal:** Demonstrates adherence to laws discouraging interactions with cybercriminals.
   - **Practical:** Recovery without payment may be slower and costlier but prevents future dependency on such negotiations.

Post-Incident Measures:

1. **Technical and Organizational Improvements:**
   - **Anti-Phishing Tools:** Deploy email filtering and detection systems to block phishing attempts.
   - **Backup Systems:** Implement automated, regular backups and test recovery processes to ensure data integrity.
   - **Endpoint Security:** Use advanced threat detection tools and endpoint protection software.
2. **Employee Training:**
   - Conduct regular training sessions to educate staff on recognizing phishing links and cyber threats.
   - Simulate phishing scenarios to evaluate and improve employee awareness.
3. **Incident Response Plan:**

   - Develop a plan aligned with the **Computer Misuse Act** to address and mitigate future cyberattacks.
   - Include steps for containment, recovery, reporting, and external communication during incidents.
4. **Collaboration with Authorities:**
   - Report the incident to law enforcement and relevant regulatory bodies to ensure transparency.
   - Engage cybersecurity experts for forensic investigations and secure guidance.
5. **Policy and Infrastructure Updates:**
   - Enforce multi-factor authentication (MFA) and least-privilege access policies.
   - Regularly update software and systems to patch vulnerabilities.
6. **Public Relations Management:**
   - Communicate transparently with customers about the breach, steps taken, and measures to prevent recurrence.
   - Offer support services such as credit monitoring for affected customers.

By refusing to negotiate where feasible, strengthening cybersecurity measures, and adhering to legal frameworks like the Computer Misuse Act, the company can mitigate risks and build resilience against future attacks.

How can the company protect its intellectual property, and what legal measures can it take against the competitor?

- **File for Patents:** Protect unique algorithms, processes, or innovations through patent filing after conducting a patent search.
- **Register Copyrights:** Secure software code and UI/UX designs through copyright registration for stronger protection.
- **Protect Trade Secrets:** Use non-disclosure agreements (NDAs) and implement security measures to keep proprietary technology confidential.
- **Cease-and-Desist Letter:** Send a formal letter to competitors to stop alleged patent or copyright infringement.
- **Negotiate or Settle:** Resolve conflicts through licensing agreements or negotiations before considering litigation.
- **Take Legal Action:** File lawsuits for patent infringement or breach of confidentiality if necessary.
- **Secure Development Process:** Strengthen security measures to prevent further source code leaks and restrict access to sensitive information.
- **Pursue Legal Action for Leaks:** Take disciplinary or legal action against team members responsible for code leaks.
- **Monitor Competitors:** Continuously check the market for potential infringement or unauthorized use of intellectual property.

Question (Patents): A tech company has developed a new smartphone with a unique camera feature. A competitor claims that the feature infringes on its existing patent. The tech company believes the patent is invalid. How should the tech company proceed to address the patent infringement claim and protect its innovation?

- **Review the patent**: Analyze the competitor's patent to determine if the feature truly infringes on it.
- **Seek legal counsel**: Consult with an IP attorney to evaluate the validity of the competitor's patent and whether the tech company's feature violates it.
- **Challenge the patent**: If the patent appears invalid or overly broad, consider filing for a patent invalidation or opposition.
- **Negotiate**: Attempt to settle the dispute through licensing, a cross-licensing agreement, or other terms with the competitor.
- **Alternative designs**: If the patent is valid, explore options to modify the feature to avoid infringement.
- **File for a patent**: Ensure the tech company's innovation is well-protected by applying for a patent if not already done.
- **Document everything**: Keep detailed records of all communications, design processes, and actions taken to protect the innovation.

A company collects personal data from customers for a loyalty program. However, it later discovers that the data was shared with a third-party vendor without the customers' consent. How should the company address the breach, notify affected customers, and ensure compliance with data protection laws like GDPR?

 Acknowledge the breach:

- Identify and assess the extent of the breach.
- Determine which personal data was shared and the potential risks to customers.

 Notify affected customers:

- Inform customers about the data breach as soon as possible, detailing what data was shared, how, and the potential risks.
- Provide customers with steps they can take to protect their data (e.g., changing passwords, monitoring accounts).

 Notify regulatory authorities:

- Under GDPR, notify the relevant data protection authority within 72 hours if the breach poses a risk to customer privacy.

 Investigate the cause:

- Conduct an internal investigation to understand how the breach occurred and why customers' consent was not obtained.
- Review and update internal data protection practices and agreements with third-party vendors to prevent future breaches.

 Enhance data protection practices:

- Implement stricter consent processes for sharing customer data, ensuring customers are informed and their consent is properly obtained.
- Review vendor contracts to ensure they comply with data protection laws and require strong security practices.

 Monitor and report:

- Continuously monitor for any misuse of the exposed data.
- Consider offering affected customers identity theft protection or other remedial actions.

A company is developing a new mobile app that collects personal data from users. The company plans to store this data in a cloud-based system. What steps should the company take to ensure compliance with data protection regulations (e.g., GDPR) and protect user privacy?

Conduct a Data Protection Impact Assessment (DPIA):

- Assess potential risks to user privacy and data protection before launching the app.
- Evaluate how the data will be collected, processed, stored, and shared.

Obtain Explicit Consent from Users:

- Ensure that users give informed, explicit consent for data collection.
- Provide clear, transparent information on what data is collected, the purpose, and how it will be used.

Minimize Data Collection (Data Minimization Principle):

- Only collect the necessary data required for the app's functionality.
- Avoid collecting excessive or irrelevant data.

Ensure Data Security:

- Implement robust encryption mechanisms to protect data both in transit and at rest.
- Use secure authentication methods (e.g., multi-factor authentication) to protect user accounts.

Implement User Rights:

- Allow users to easily access, correct, or delete their personal data.
- Provide an option to withdraw consent at any time.

Establish Clear Data Retention Policies:

- Define how long user data will be stored and ensure it is not kept longer than necessary for the app's purpose.

Ensure Third-Party Compliance:

- Review the data protection practices of any third-party service providers (e.g., cloud storage services) to ensure they comply with relevant laws and regulations.
- Sign data processing agreements with third parties to outline their obligations and responsibilities.

Maintain Transparency and Privacy Notices:

- Provide a clear privacy policy and terms of service that explain how user data is handled.
- Update the policy regularly to reflect any changes in data practices.

Implement Data Breach Protocol:

- Have a plan in place to detect, report, and respond to data breaches.
- Notify users and regulatory bodies within the required time frame if there is a data breach involving their personal information.