Ethics and Professionalism in Computing

Chapter 1: Introduction

What's Ethics?

- Means `custom`, `habit`, and `way of living`.
- Principles of right or wrong.
- The rules or standards governing the conduct of a person or the members of a profession.
- Standards of conduct that indicate how one should behave based on moral duties and virtues.
- Derived from principles of right and wrong and concerned with human conduct.
- Behaviour of individuals in society.
- A system of morals of a particular person, religion or a group.
- Studies:
  - The general nature of morals.
  - The specific moral choices to be made by a person
  - Moral philosophy
- Guidelines established by communities or specific groups outlining acceptable and unacceptable actions or behaviours.
- `Ethical theory` is a system of ethics guiding towards actions good for all.

What's Moral?

- Dealing with, or capable of, distinguishing between right and wrong, and between just and unjust.
- Personal belief influenced by factors such as society, culture, and individual experiences.

Ethics vs Morals

Morality	Ethics
1. More general and prescriptive based on customs and traditions.	1. Specific and descriptive. It is a critical reflection on morals.
2. More concerned with the results of wrong action, when done.	2. More concerned with the results of a right action, when not done.
3. Thrust is on judgment and punishment, in the name of God or by laws.	3. Thrust is on influence, education, training through codes
4. In case of conflict between the two, morality is given top priority, because the damage is more. It is more common and basic.	4. Less serious, hence second priority only. Less common. But relevant today, because of complex interactions
5. Example: Character flaw, corruption, extortion, and crime.	5. Example: Notions or beliefs about manners, tastes, customs, and towards laws

Applied Ethics

- The practice of ethics.
- Rules for ethical behaviour for everyday life.
- Impossible for all people to share same applied ethics in all details.

Factors that determine how one decide ethical issues

- The set of practical circumstances involved in the decision that one is trying to make.

Josephson's Core Values Model

- Recognize that there is a decision that involves ethical judgment.
- Ask as many questions as are necessary to get a full background on the relevant facts(have all the needed information).
- **Steps**:
  - `Identify stakeholders` : who are the potential gainers and losers in the various decisions that might be made here?
  - Identify several likely or reasonable decisions that could be made.
  - Consider which stakeholders gain or lose with each decision.
  - Determine which decision satisfies the greatest number of core values
  - Otherwise, try to determine which decision delivers the greatest good to the various stakeholders
- **Core values**:
  - Trustworthiness:
    - Be honest
    - Demonstrate integrity
    - Keep promises
  - Respect
  - Responsibility:
    - Be accountable
    - Pursue excellence
  - Fairness
  - Caring
  - Citizenship

Profession

- A calling that requires specialized knowledge and long, intensive academic preparation.
- Social mechanism for managing expertise and deploying it in ways that benefits society.
- It is not individual basis, societies choose to recognize professions.
- Not about salaries or social status, it is about being `strongly differentiated` .
- **Characteristics**:
  - `Mastery of a secret body of knowledge` :
    - Abstract and systematic.
    - Can be mastered only through disciplined study typically in higher education.

- `Autonomy` : highlights the difference between working autonomously (self-directed) and working under close supervision (externally directed).
- `Formal organization` : single unifying organization recognized by regional and/or national governments,to specify criteria for licensing members and power to expel individual members from profession.
- `Code of Ethics` : code of professional conduct, public statement for public, a formal specification of special contract.
- `Culture of practice` : distinctive culture.
- `Social contract with society` : a system of trust.

Professional Ethics

- Concerns one's conduct of behaviour and practice when carrying out professional work.
- Introduced by professional organization to individuals.
- **Importance**:
  - `Complex Relationships` : Professionals often navigate interactions with people of varying levels of expertise, such as clients or colleagues who may have limited technical knowledge.
  - `Social Dynamics` : Success in a professional setting involves managing relationships with diverse stakeholders, including clients, employers, and coworkers.
  - `Adherence to Principles` : Employees are expected to strictly follow ethical principles, which are non-negotiable in professional contexts.
  - `Discipline and Decorum` : Adhering to these principles promotes discipline and ensures a respectful and orderly workplace.
  - `Key Ethical Values` : Values such as confidentiality, fairness, transparency, and proficiency are essential for fostering trust and accountability.
  - `Responsibility` : Following ethical guidelines helps employees take responsibility for their actions and decisions, contributing to a more professional and reliable work culture.
- **Types**:
  - Meta ethics: (origin of ethical principle):
    - It deals with origin of ethical principles that govern the specification of right and wrong behaviour.
    - A major issue of debate in this category is whether ethical principles are eternal truths that evolved from a spiritual world or simply created by the humans.
  - Descriptive ethics: (moral beliefs):
    - It refers to the study of moral beliefs of the people.
    - It is a field of empirical research into what people or societies consider right or wrong.
  - Normative ethics: (self moral conduct):
    - It is concerned with arriving at set of moral conduct rules against which behaviour are judged.
  - Applied ethics:
    - Principles designed or written for implementation in a specific situation.
    - `Bio ethics` , `Medical ethics` , `Computer ethics` , `Engineering ethics` , `Business ethics` , and `Legal ethics` .

- **Features**:
  - `Openness` , `Transparency` , `Privacy` , `Impartial` , `Practical and un-biased` , `Loyal` , `Co-operative` , `Objective oriented` .

Accounts of professional Ethics

- **Conflicting responsibilities**:
  - `When to Act` : Deciding when to take a stand (“rock the boat”) or expose wrongdoing (“blow the whistle”) in situations involving ethical conflicts or harm.
  - Types of Ethical Conflicts:
    - Working on projects that conflict with personal beliefs or ethical standards.
    - Balancing the need for income or contracts with the moral implications of a project’s outcomes.
    - Addressing clients’ willingness to compromise on safety or security.
  - `Whistleblowing` :
    - Taking the step to disclose harmful practices or situations after internal channels have failed.
    - Recognizing whistleblowing as a serious decision, often involving breaking organizational norms to uphold ethical integrity.
    - **DeGeorge’s 5 questions (ask your self before)**:
      - `Have Right` :
        - Do you believe the problem may result in “serious and considerable harm to the public”?
        - Have you told your manager your concerns about the potential harm?
        - Have you tried every possible channel within the organization to resolve the problem?
      - `Have Duty` :
        - Have you documented your evidence that would persuade a neutral outsider that your view is correct?
        - Are you reasonably sure that if you bring this matter to public attention, something can be done to prevent the anticipated harm?
  - `Gun for hire argument` :
    - This approach is characterized by a focus on performing tasks for clients without considering the broader ethical or societal implications, as long as the work is legal and profitable.
    - Prioritizes expertise as a service, leaving the purpose or consequences of the work to the client.
    - The belief is that as long as the work complies with the law, no ethical issues arise.
    - Risks:
      - Can lead to quick, cost-driven solutions that prioritize market demands over quality, security, or ethics.
      - Professionals might inadvertently facilitate unethical or harmful outcomes, such as fraud, due to a lack of accountability for the end use of their work.
  - `Efficacy` : responsibility for safe and reliable computing for the sake of society and computer professionalism.

    - Moral responsibilities:
        - `Role responsibility` : assigned duties.
        - `Casual responsibility` : action or inactin cause harm.
        - `Legal responsibility` : assigned by law.
    - Moral responsibility is not exclusive and “If whistleblowing should be done, and no individual has the strength to do it, then it must be done by a group acting collectively.” (Micheal McFarland).
- **Professionals and other stakeholders(Society)**:
    - Professional activities can influence individuals or groups who are not directly involved, such as the public or end-users.
    - The consequences of professional work often extend beyond the immediate scope of the project.
    - Laws cannot foresee or regulate all potential effects of professional actions, especially in complex or rapidly evolving fields. Therefore ethical responsibility fills the gaps where legal guidelines are absent or insufficient.
- **Employee and employer**:
    - The relationship is initially defined by `written terms` such as `job responsibilities` , `salary` , and `working hours` .
    - There are also unwritten or assumed expectations, which may not be explicitly discussed but are often implied, such as:
        - Adhering to legal and company rules.
        - Being flexible with work, such as putting in overtime when needed.
        - Avoiding actions like public speaking that could reflect negatively on the employer.
        - Accepting assignments, even if they conflict with personal beliefs.
    - Kant’s categorical imperative:
        - Employee provides labour, employer provides compensation.
        - No party treats other as means to an end.
        - Both must be honest.
    - `Manipulation` : using dishonesty to manipulate others reduces individuals to tools for achieving specific goals, ignoring their inherent value and rights.
    - `Workplace Hazards` : ethical concerns arise when employers exploit employee vulnerabilities, withhold benefits or salaries, fail to disclose risks, or treat employees as mere resources rather than individuals deserving respect and fairness.
    - `Loyalty` :
        - Positive loyalty involves commitment to the organization or ethical practices.
        - Negative loyalty includes favoritism (e.g., hiring friends) or misuse (e.g., exploiting loyalty for self-serving activities like vote-routing or product enforcement).
    - `Trade Secrecy` : protecting company secrets is often a key part of professional responsibilities, but it raises challenges when an employee’s expertise, considered their only asset, conflicts with restrictive agreements like non-compete clauses upon resignation.
- **Professionals and clients**:
    - Clients rely on professionals for their specialized knowledge and expertise due to their lack of understanding in the field.
    - Trust is central to this relationship.

    - Models:
        - `Agency Model` : The professional acts strictly according to the client's instructions, with minimal autonomy (e.g., stockbrokers).
        - `Paternalistic Model` : The professional assumes full control, making decisions on behalf of the client (e.g., traditional doctor-patient relationship).
        - `Fiduciary Model` : Both the professional and client share roles and responsibilities, requiring mutual trust and collaboration.
- **Professionals and professional**:
    - Loyalty can involve protecting colleagues, avoiding public criticism, and supporting each other in career advancement. However, this loyalty can have both positive and negative aspects, as excessive or blind loyalty might conflict with broader ethical responsibilities.

Ethical Theories and Frameworks Applied to Computer Ethics

- **Utilitariansim**:
    - A consequentialist ethical theory that focuses on maximizing overall happiness or well-being.
    - Can be applied in computer ethics to assess the consequneces of technology use and determine whether it benefits the greatest number of people.
- **Dentology**:
    - A non-consequentialist ethical theory that emphasizes the inherent rightness or wrongness of actions based on a clear set of rules, irrespective of their outcomes.
    - Can be applied in computer ethics to guide ethical decision making by focusing on principles and rules.
- **Virtue Ethics**:
    - Centred around cultivating moral character traits and virtues.
    - Can be applied to computer ethics to focus on developing ethical virtues in individuals working with technology, such as `honesty` , `integrity` , and `responsibility` .
    - It encourages professionals to act in ways that demonstrate good character and promote ethical behaviour in their technological practices.
- **Rights-Based Ethics**:
    - Asserts that individuals have certain fundamental rights the must be respected.
    - Can be applied in computer ethics to identify and protect digital rights, such as the `right to privacy` , `freedom of expression` , and `access to information` .
    - Provides a foundation for defending individuals' rights in the face of emerging digital challenges.
- **Social Contract Theory**:
    - Suggests that ethical principles and rules arise from a social agreement among individuals to promote cooperation and societal well-being.
    - Can be applied to computer ethics:
        - By establishing rules and regulations concerning the responsible use of technology and data.
        - On obligations of technology developers and users towards society.

- **Feminist Ethics**:
  - Focuses on the values of `care`, `empathy`, and `rationality`.
  - Can be applied to computer ethics by highlighting the importance of considering the needs and perspectives of all stakeholders particularly those who might be marginalized or disproportionately affected by technology.
  - Advocates for a more inclusive and empathetic approach to technological development and deployment.
- **Ethical Pluralism**:
  - Acknowledges that different ethical theories may offer valuable insights and that no single theory can address all ethical dilemmas comprehensively.
  - Can be applied to computer ethics to encourage a holisitc approach that considers multiple ethical perspectives when making complex decisions related to technology.
- **Ethical of Prudence**:
  - Emphasizes the importance of precautionary measures and risk assessment when dealing with uncertain or potentially harmful technologies.
  - Can be applied to computer ethics to guide the consideration of long-term consequences and potential risks associated with new technological advancements.
- **Precautionary Principle**:
  - Advocates for taking preventive actions to avoid harm even in the absence of scientific certainity.
  - Often applied to emergin technologies where the potential risks may not be fully understood.
  - Calls for ethical caution and prudence when deploying such technologies.
- By applying these ethical theories and frameworks, computer ethics professionals and stakeholders can:
  - Engage in informed ethical discussions,
  - Assess the impact of technology on society, and,
  - Make responsible decisions that align with moral values and principles.

Software Engineering

- Focuses on `Specification`, `Development`, `Validation`, and `Evolution`.
- Software engineering is more of a craft, based on trial and error, rather than on calculation and prediction.

Reliability and safety of Computer Systems

- Computers and software differ from regular machine-elements on two key issues:
  - They have a discontinuous behaviour.
  - Software lack `physical restrictions` and `structure` or `function` related attributes.
- The sole physical entity that can be modelled and measured by software engineers is `time`.
- Software's flexibility is both an advantage and a challenge. While its adaptability allows for easy changes and complex designs, this lack of physical constraints leads to increased complexity.

This complexity, in turn, becomes a major source of design faults, as unanticipated interactions between components make it harder to predict and manage all possible behaviors.

- Software is a product of intellectual effort and is inherently prone to flaws due to human imperfections, unlike physical systems affected by material defects. Faulty software can lead to failures when it cannot meet its specifications, resulting in crashes, errors, hangs, or incorrect outputs. The reliability of software decreases as the failure rate increases.

- Other issues:

  - `Reliability` is the probability that a piece of equipment or component will perform its intended function satisfactorily for a prescribed time and under stipulated environmental conditions. It is often quantified by `MTTF – Mean Time To Failure .`
  - `Availability` is the probability that the system will be functioning correctly at any given time. It is usually quantified by `MTTR/MTTF` , where MTTR is the `mean time to repair the system` and MTTF the `mean time to failure .`
  - `Failure` is the non-performance or inability of the system or component to perform its intended function for a specified time under specified environmental conditions. It is a behaviour or an event.
  - `Error` is a design flaw or deviation from a desired or intended state.
- **Causes of failure**:

  - Fault in requirement and design specifications.
  - Faults introduced in the design and implementation phases
  - Faults in the hardware
  - Mistakes by the operator
- **Nature of software and its environment**:

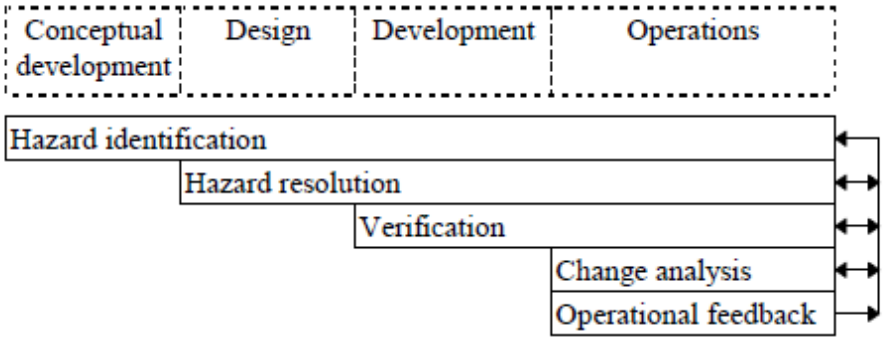
  - Achieving and assessing `reliability` and `safety` is hard.
  - Software with pure design is deterministic.
  - If an error is afflicting the software, it will always lead to a failure if the wrong circumstances arise.
  - The occurrence of a specific event or circumstance in a system is not predictable in a straightforward, cause-and-effect manner. Instead, it is influenced by random or probabilistic factors (a stochastic process):
    - `Non-deterministic` : The outcome is not fixed or certain; the system's behavior depends on variables that can change unpredictably.
    - `Sequence of Inputs and Interactions` : The system's responses are shaped by a combination of inputs it receives and its interactions with the environment, which may vary over time.
    - `Stochastic Process` : This refers to a process that incorporates randomness, meaning that the sequence of events unfolds according to probabilities rather than a predetermined path.
- **Construction of Dependable Systems**:

  - Laprie's approaches:
    - `Fault avoidance` :

    - Implies the set of methods used for producing programs that are, by design free of faults.
    - Use of `formal methods`, `semi-formal methods`, `structured methods` and `object-oriented methods`.
    - Impose discipline and restrictions on the designers of a system.
    - Introduce virtual physical laws that hinders the designers from making too complex designs and provide means to model and predict the behaviour of their designs.
    - Supply the computer software engineers with mathematical logic and discrete mathematics as a tool to model their designs.
- `Fault Removal`:
    - Implies the set of methods used to remove faults from existing programs.
    - Includes the combined use of `formal specification` and `dynamic verification` (`experimentation`, `dynamic testing`, and `testing`).
- `Fault Tolerance`:
    - The ability to continue operating despite failures or malfunctions.
    - Has also been applied to accommodate for design deficiencies.
    - Methods:
        - `Robust designs`:
            - Aims to ensure that a software system can continue to operate correctly or gracefully handle unexpected inputs, conditions, or failures.
            - `Key characteristics`:
                - Error Handling: Implementing mechanisms to detect and recover from errors without crashing the system.
                - Graceful Degradation: Allowing the system to maintain partial functionality instead of complete failure during faults.
                - Defensive Programming: Writing code that anticipates and safely handles potential issues, such as invalid inputs or resource unavailability.
                - Boundary Testing: Ensuring the system behaves predictably under extreme or edge conditions.
                - Input Validation: Verifying and sanitizing inputs to prevent faults caused by invalid or malicious data.
        - `Redundant designs`:
            - Incorporate extra components or systems to provide backups in case of failure.
            - `Key characteristics`:
                - Replication: Duplicating critical components or subsystems (e.g., multiple servers or processes) so that if one fails, another can take over.
                - Diversity: Using different implementations of the same functionality to reduce the risk of common-mode failures (e.g., employing diverse algorithms or coding teams).

        - Failover Mechanisms: Automatically switching to a redundant system or component when a failure is detected.
        - Checkpointing: Regularly saving the system's state so it can recover from failures without losing progress.
        - Voting Systems: Implementing multiple redundant systems that compare outputs and use a majority-vote mechanism to decide the correct result (e.g., in critical systems like flight controls).
- **Distinctions between reliability and safety**:
    - `Safety` : considers the consequences of failures, especiallt the failures that lead to hazards.
    - `Reliability` : only quantifies the frequency of failures disregarding the consequence of a failure.
- **Test and specifications**:
    - The intention of testing is often to verify that a specific input will yield a specific output, defined by the specification.
- **Software and hazards**:
    - Software will be hazardous when executed on a computer, but even then there exists no real danger.
    - Hazard occur when the computer and the software starts monitoring and controlling physical components.
    - Tasks:
        - `Development` : the examination of a new system to identify and assess potential hazards and eliminate and control them.
        - `Operational management` : The examination of an existing system to identify and assess hazards in order to improve the level of safety.
        - `Certification` : the examination of the planned and/or existing system to demonstrate its level of safety and to be accepted by the customer, authorities or the public.
        - The two first tasks are intended to make the system safer, while the third task has the goal of convincing management and government that the system is safe.
        - Steps:
            - `Define scope` : which components and data that are to be subjected to the analysis.
            - Identify hazards that singly or in combination could cause an accident.
            - Rank the hazards in order to know, which hazard to attack first.
            - Evaluate the causal factors related to the hazards:
                - Determine how the hazards could occur, their nature, and their possible consequences.
                - Examine the interrelationships between causal factors.
            - Identify safety design criteria, safety devices, or procedures that will eliminate or minimize and control the identified hazards.
            - Find ways to avoid or eliminate specific hazards.

        - Determine how to control hazards that cannot be eliminated and how to incorporate these controls into the design.
        - Evaluate the adequacy of hazard controls.
        - Provide information for quality assurance:
            - Quality categories, required acceptance tests and inspections, and items needing special care.
        - Evaluate planned modifications.
        - Investigate accidents and near-miss reports.
            - Determine whether they have validity and, if they do, the cause of the problem.
        - Certification of the system:
            - Demonstrate the level of safety achieved by the design.
            - Evaluate the threat to people from the hazards that cannot be eliminated or avoided.
- **The iterative hazard analysis process**:
    - Hazard analysis is both iterative and continous over time.
    - Begins with hazard identification during the conceptual phase of the system and continues in through out the construction and operation of the system.



    - Hazard identification:
        - Continually updated with new information about new and old hazards.
        - Process continues through the entire lifetime of the system.
        - The output is used in developing:
            - System safety requirements
            - Preparing performance
            - Resource and design specifications
            - Test planning
            - Preparing operational instructions, and management planning.
        - `Ranking hazards`:
            - Helps to prioritize hazards so a sound judgment can be made regarding in which order hazards should be eliminated, reduced or ignored.
        - `Hazard consequences`:

Catastrophic:	People	;death.
	Facilities	;system loss, cannot be repaired, requires salvage or replacement.
	Environment	;severe environmental damage.
Critical:	People	;severe injury/illness; requires medical care (lengthy convalescence and/or permanent impairment)
	Facilities	;major system damage, loss of mission
	Environment	;major environmental damage.
Marginal:	People	;minor injury/illness; requires medical care but no permanent impairment.
	Facilities	;loss of non-primary mission
	Environment	;minor environmental damage.
Negligible:	People	;superficial injury/illness; little or no first aid treatment
	Facilities	;less than minor system damage; disabled less than one day.
	Environment	;less than minor environmental damage.

Frequent	-Likely to occur frequently during system's life time.
Probable	-Will occur several times during system's life time.
Occasional	-Likely to occur sometime during system's life time.
Remote	-Unlikely to occur during system's life time.
Improbable	-Extremely unlikely to occur during system's life time.
Impossible	-Probability equal to zero.

- `Casual factors` :
  - When hazards have been identified the next step is to conclude what causes and effects are associated with each hazard.
  - It is necessary to trace backwards, from effect to cause, and from effect to cause, and so on.
  - A cause is a set of circumstances or events that are sufficient for a certain effect to occur.
- `System hazard analysis` : consider the system as a whole and identifies the behavior of the system relating to the interface between components and how the interface between the system and the operator can contribute to hazards.
- `Subsystem hazard analysis` : consider the individual subsystems' operating and failure modes impact on the system hazards.
  - Typical subsystems are:
    - Power – electricity, pneumatic pressure,
    - Control – computers and software
    - Operators, Communication – Computer networks
    - Sensors, Actuators
    - Propulsion – Engines, Gas,…
  - This analysis evaluates: primary faults, secondary faults (faulty input) and command faults (timing issues).
  - Methods of identifying cause of hazard:
    - Checklists
    - `Fault Tree Analysis (FTA)` :

        - A method for finding causes of hazards, not identifying hazards.
        - Tries to reduce the number of behaviours that need to be considered in order to get assurance that the design is safe.
        - An analytical method using proof by contradiction.
        - Analyzes the system top-down to find paths leading to the hazard.
        - Uses Boolean logic to represent how faults combine to cause the hazard.
        - Takes preventive actions if causes are identified; otherwise, the hazard cannot occur.
        - Quantifies hazard probability using fault tree analysis (FTA), but some causes (e.g., design errors) may not be measurable.
        - More effective for qualitative analysis than for precise probability estimation.
    - Event Tree analysis – ETA
    - Cause Consequence Analysis – CCA
    - Hazards and Operability Analysis – HAZOP
    - Failure Modes and Effects Analysis – FMEA
    - Failure Modes, Effects and Criticality Analysis – FMECA
    - Fault Hazard Analysis – FHA
    - State Machine Hazards Analysis – SMHA

Professional Code of Ethics

- Software engineers, as per IEEE-CS/ACM guidelines, should uphold ethics by ensuring software analysis, design, development, testing, and maintenance benefit society and elevate the profession's reputation.
- In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:
    - `PUBLIC` : act consistently with the public interest.
    - `CLIENT AND EMPLOYER` : act in a manner that is in the best interests of their client and employer consistent with the public interest.
    - `PRODUCT` : ensure that their products and related modifications meet the highest professional standards possible.
    - `JUDGMENT` : maintain integrity and independence in their professional judgment.
    - `MANAGEMENT` : as managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
    - `PROFESSION` : advance the integrity and reputation of the profession consistent with the public interest.
    - `COLLEAGUES` : be fair to and supportive of their colleagues.
    - `SELF` : participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.
- The computer ethicists Martin and Martin made a comparison of the ethical codes of four computer societies `ACM code of Ethics and other Codes` , `Institute of Electrical and Electronics Engineers (IEEE)` , `Data Processing Managers Association (DPMA)` and, `Institute for the Certification of Computer Professionals (ICCP)` .

- They found ten common themes that emerged as the core for ethical behaviour for computer professionals:
    i. Personal integrity/claim of competence
    ii. Personal responsibility for work
    iii. Responsibility to employer/client
    iv. Responsibility to profession
    v. Confidentiality of information
    vi. Conflict of interest
    vii. Dignity/worth of people
    viii. Public safety, health, and welfare
    ix. Participation in professional societies
    x. Increasing public knowledge about technology
- These ten universal common themes are referenced in an ethical analysis.
- The second principle to be referenced under Formal Guidelines is extracted from Confucianism.
- `Confucianism`：
    - Ethical system of the Chinese philosopher Confucius (551-479 BC).
    - Sometimes summed up in the rule.
    - ‘What you do not want others to do to you, do not do to them.’.
    - Also known as the Golden Rule.

Chapter 2: Privacy

What’s Privacy?

- Refers to the ability of individuals to control their personal information and to prevent unwanted intrusion or exploitation.

What’s Information?

- It is an intangible product that is transmitted through media.
- Information is the result of processing, manipulating and organizing data, which is simply a collection of facts.
- Information can be defined as an “asset”.

Information Assets vs Physical Assets

Characteristics	Information Assets	Physical Assets
Form-maintenance	• Have no physical form and can be flexible	• Have physical form
Value-variableness	• Attain higher value when combined and processed	• Total value is the sum of each value
Sharing	• Unlimited reproduction of information assets is possible, and people can share the value	• Reproduction is impossible; with reproduction, the value of the asset is reduced
Media – dependency	• Need to be delivered through media	• Can be delivered independently (due to their physical form)

Risks to Information Assets

- Increase in unethical behaviour arising from anonymity
- Conflicts over ownership and control of information
- Information and wealth gaps between classes and countries
- Growing information exposure caused by advanced networks

Information Security

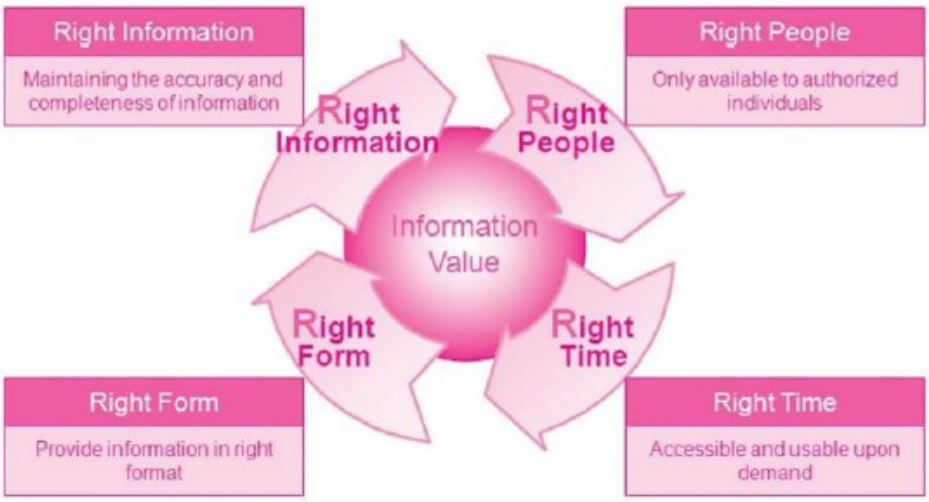
- The preservation of `confidentiality`, `integrity` and `avaliability` of information.
- Involves preventing or at least reducing the probability of `unauthorized/inappropriate access`, `use`, `disclosure`, `disruption`, `deletion/destruction`, `corruption`, `modification`, `inspection`, `recording` or `devaluation` of information.
- Reducing the adverse impacts of incidents.
- Focus on the balanced protection of the `confidentiality`, `integrity` and `availability` of data (also known as the CIA triad).
- Maintain a focus on efficient policy implementation, all without hampering organization productivity.

Cyber Security

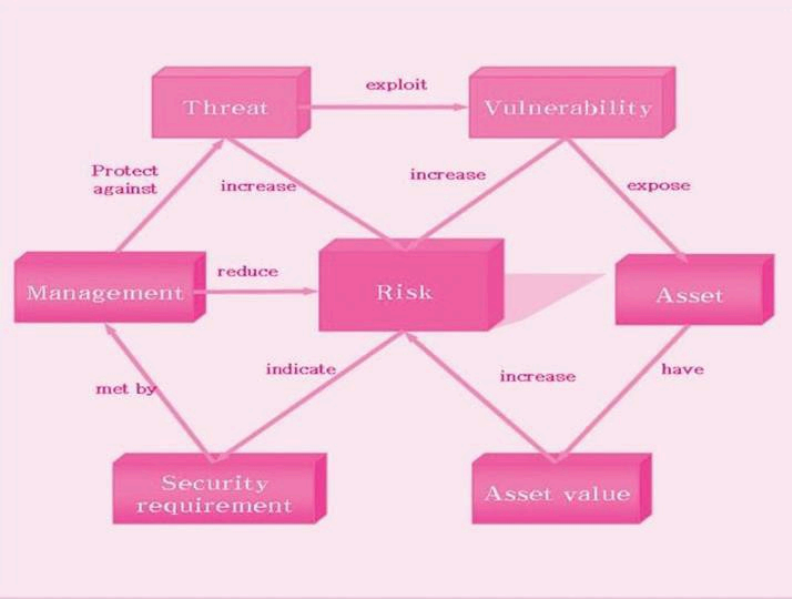
- Includes not only information security, but also digital infrastructure security like Supervisory Control and Data Acquisition (SCADA) systems and Internet-of-Things (IoT) systems.
- Goes beyond the protection of valuable information.

4Rs of information security

- `Right Information`, `Right People`, `Right Time`, and `Right Form`.

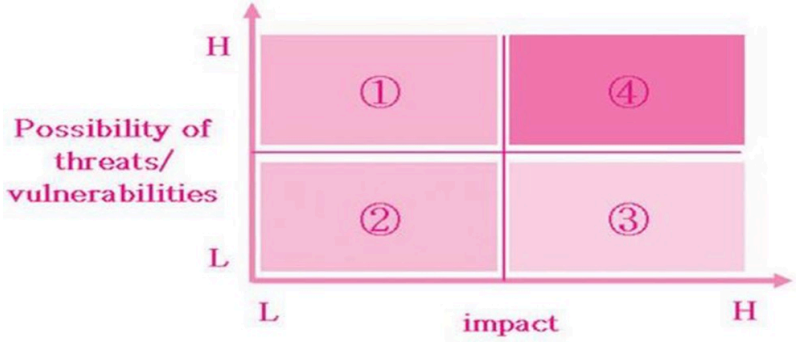


- To safeguard information security, the 4Rs have to be applied properly and `confidentiality`, `integrity` and `availability` should be observed when handling information.



Risk Management

- Risk is determined by the `asset value`, `threats` and `vulnerabilities`.
- This risk can be increased or decreased by manipulating the size of the asset value, threats and vulnerabilities.
- **Methods**:
  - Risk reduction (risk mitigation):
    - This is done when the likelihood of `threats/vulnerabilities` is `high`, but their `effect` is `low`.
    - It involves understanding what the threats and vulnerabilities are, altering or reducing them, and implementing a countermeasure.
    - However, risk reduction does not reduce the value of risk to 0.
  - Risk acceptance:
    - This is done when the likelihood of threats/vulnerabilities is low and their likely impact is minor or acceptable.
  - Risk transference:
    - If the risk is excessively high or the organization is not able to prepare the necessary controls, the risk can be transferred outside of the organization. An example is taking out an insurance policy.
  - Risk avoidance:
    - If the threats and vulnerabilities are highly likely to occur and the impact is also extremely high, it is best to avoid the risk by outsourcing data processing equipment and staff.



Standards for Information Security Activities

- **Examples**:
  - The International Organization for Standardization and International Electrotechnical Commission (ISO/IEC).
  - International Telecommunication Union (ITU-U).
  - Information security requirements and evaluation items of the Certified.
  - Information Systems Auditor (CISA) of the Information Systems Audit and Control Association (ISACA).
  - Certified Information Systems Security Professional (CISSP) of the International Information System Security Certification Consortium (ISC)2
- These standards recommend unified information security activities, such as:
  - The formulation of an information security policy
  - The construction and operation of an information security organization,
  - Human resources management,
  - Physical security management,
  - Technical security management,
  - Security audit and business continuity management.

The concept of privacy

- Personal information is any information relating to an identifiable individual or an identified or identifiable natural person.
- Personal information includes `name`, `phone number`, `address`, `e-mail address`, `licence number of an automobile`, `physical characteristics` (`facial dimensions`, `fingerprints`, `handwriting`, etc.), `credit card number` and `family relationship`.
- The focus is on protecting an individual's right to control their personal information rather than merely safeguarding the data itself.

Five ways to explain the right to privacy

1. The right to be free from unwanted access (e.g., physical access and access via short messaging service)
2. The right not to allow personal information to be used in an unwanted way (e.g., sale of information, exposure of information and matching)
3. The right not to allow personal information to be collected by others without one's knowledge and consent (e.g., through the use of CCTV and cookies)
4. The right to have personal information expressed accurately and correctly (i.e. integrity)
5. The right to get rewarded for the value of one's own information

The Passive and Active concepts of privacy

- **Passive concept**:
  - Focuses on protecting individuals from external interference or intrusion.
  - It is about ensuring people can live their lives without unwanted disturbances or invasions of their personal space.

    - `Right to be let alone`, `Dignity of human beings`, and `Legal connection`.
- **Active concept**:
    - Emphasizes an individual's ability to actively manage, control, and make decisions about their personal information.
    - It's about giving individuals agency over how their data is used.
    - `Self control of personal information`, `Right to correct information`, and `Positive management`.

OECD principles

- Outline the rights and obligations of individuals in the context of automated processing of personal data, and the rights those who engage in such processing.
- Applicable at `national`, `international`, `public`, and `private` sectors.
- **Principles**:
    - Collection limitation principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
    - Data quality :
        - `Personal data`:
            - Should be relevant to the purposes for which they are to be used and, the extent necessary for those purposes,
            - Should be accurate, complete and up-to-date.
    - Purpose of specification principle:
        - It ensures that personal data is collected and used responsibly and transparently.
        - The purposes for which personal data are collected should be specified not later than at the time of data collection.
    - Use limitation principle:
        - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle except with the consent of the data subject or by the authority of law.
    - Security safeguards principle:
        - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
    - Openness principle:
        - There should be a general policy of openness about developments, practices and policies relating to personal data.
        - Individuals should have clear and accessible information about their data, its use, and who is responsible for it.
    - Individual participation principle:
        - An individual should have the right to:
            - Obtain from a data controller confirmation of whether the data controller has data relating to him/her;
            - Receive communication about data relating to him/her within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that

is readily intelligible to him/her;
        - Be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
        - To challenge data relating to him/her and, if the challenge is successful, to have the data erased, rectified, completed or amended.
    - Accountability principle:
        - A data controller should be accountable for complying with measures that give effect to the principles stated above.

UN guidelines related to protection of privacy

- The United Nations Guidelines are applied to documents (papers) as well as computerized data files in the public or private sectors. – The Guidelines establish a series of principles concerning minimum guarantees to be provided for national legislation or in the internal laws of international organizations.

Computer Crime

- **Nature and Scope of Cyber Crime**:
    - Crime is a socially correlated phenomenon.
    - Crimeless society is a myth and crime cannot be segregated from a society.
    - Thus the nature of the crime depends upon the nature of a society.
    - Complexity of the society determines the complexity of the crime that evolves' around it.
- **Factors which influence and contribute to the crime**:
    - The socio-economic and political structure of the society.
    - The preventive and corrective measures adopted by the mechanism to control the crime.
    - Criminal behaviours in the society are also taken into consideration.

Cyber Crime

- Any criminal activity which takes place on or over the medium of computers or internet or other technology recognised by the Information Technology Act.
- Any illegal action in which a computer is the tool or object of the crime.
- **Characteristics**:
    - People with specialized knowledge
    - Geographical challenges
    - Virtual world
    - Collection of Evidence
    - Magnitude of crime unimaginable
- **Classifications**:
    - Cyber pornography: is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials.
    - Cyber stalking:
        - Using internet or other electronic means is used to stalk or harass an individual, a group of individuals, or an organization.

        - It includes making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft and damage to data or equipment.
        - Cyber stalking is conducted by `email`, `through internet`, and `through computer`.
    - Cyber terrorism:
        - Refers to attacks on the computers, networks and network grids of the country which heavily depend on networks and create havoc or fear among the minds of its citizens.
        - `Objectives`:
            - Attacking a nation, a place and an organization,
            - Destroy tangible property or assets and
            - Killing human beings to prove their agenda or political ideologies.
        - `Pure cyber terriorism`: through the use of computer technology and the Internet, the terrorists seek to inflict destruction or damage on tangible property or assets, and even death or injury to individuals.
    - Hacking:
        - Unauthorized entry into a computer belonging to another individual.
        - Includes:
            - Access to a computer, Downloading.
            - Copying or extraction of data from a computer.
            - Introducing computer virus and contaminants.
            - Causing damage to a computer.
            - Causing disruption of a computer.
            - Causing denial of access to a computer.
            - Affecting critical information infrastructure.
            - Cyber terrorism.
    - Virus and Contaminants
    - Cyber crimes related to Finance
    - Phising and Vishing:
        - `Phishing` is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an instant message.
        - `Vishing` is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private, personal and financial information from the public for the purpose of financial reward.
    - Denial of Service:
        - Type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.
        - Basic types:
            - Consumption of computational resources such as bandwidth, disk space or CPU Time;
            - Disruption of configuration information, such as routing information;
            - Disruption of physical network components
        - `Distributed denial of service attack (DDoS)` occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually

one or more web servers.

- Data Theft:
  - Stealing of data and information through hacking and other means,
  - Ways:
    - The first unauthorized copying of data / information;
    - Making unauthorized subsequent copies;
    - Making a copy and dishonestly sending the data/information online;
    - Unauthorized copying of data / information in a floppy, C.D. or pen-drive and dishonestly taking it away;
    - Stealing the computer itself;
    - Data / Information already reside in a movable storage medium (floppy, C.D. or pen-drive) that is dishonestly taken away.
- Data Diddling:
  - Involves changing data prior or during input into a computer.
  - One of the simplest methods of committing a computer related crime but the cost can be considerable.
- Email Bombing:
  - A form of net abuse consisting of sending huge volumes of e-mail to an address.
  - Sometimes accomplished by giving the victim's e-mail address to multiple spammers.
  - Can be made worse if recipients reply to the e-mail.
- Email Spoofing:
  - Fraudulent e-mail activity.
  - Technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message.
  - Spoofing anyone other than you is illegal in some jurisdictions
  - Possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending e-mail, does not include an authentication mechanism.
- Logic Bombing:
  - Injecting a piece of malicious code embedded within a program that remains inactive until triggered by a specific event or condition.
  - These triggers can include time-based conditions or user actions.
  - Trojans that activate on certain dates are often called "time bombs".
- Internet time theft:
  - Occurs when someone unlawfully uses another person's internet access without their permission.
  - This typically involves:
    - `Unauthorized Access` : Gaining access to someone's login credentials (e.g., ID and password) to use their internet account.
    - `Manipulation or Tampering` : Misusing a computer, system, or network to charge internet usage or services to another person's account.
    - `Liability` : The perpetrator is held responsible for any damages or costs incurred due to this unauthorized use.
  - In essence, internet time theft involves exploiting another person's internet resources, often by fraudulently gaining access to their account, resulting in financial or resource

losses for the victim.
    - Domain Name violations and passing off

Software Piracy

- Copyright protects various forms of creative works, including literary, dramatic, musical, artistic works, computer programs, cinematographic films, and sound recordings.
- This protection ensures that creators have exclusive rights over the use and reproduction of their works.
- **Copyright in Digital Media**:
    - The internet has facilitated the easy and cost-effective transfer of large amounts of data, including copyrighted works.
    - Advances in compression technology have accelerated data sharing, raising concerns about unauthorized distribution.
- **Reproduction Rights and Databases**:
    - A database is a structured collection of data in cyberspace, designed for easy access and management.
    - Unauthorized reproduction of copyrighted material in electronic form or its inclusion in a database without the creator's consent infringes on the creator's rights.

Cyber crime with Mobile and Wireless Technology

- **Phreaking**:
    - The `exploration`, `experimentation`, and `exploitation` of telephone systems, often as a hobby or for practical purposes.
    - It involves studying and manipulating telephone systems, often using audio frequencies or small electronic devices to exploit their functionality.
    - Considered part of the broader hacking culture and is sometimes grouped under the "H/P culture" (Hacking/Phreaking).
    - While some phreaking activities involve illegal actions, not all are unlawful. Many phreakers approach it as a creative or exploratory hobby.
- Mobile phone theft
- Use of mobile and wireless technology in Terrorist activities
- **Rechipping and cloning of mobile phones**:
    - The International Mobile-Electronic Identity number (`IMEI`) of a digital, mobile phone provides a unique identity and was originally intended to be inviolably incorporated into the phone.
    - The change of identity is called `re-chipping` and can be achieved on analogue phones in a number of ways.
    - Sometimes, the `ESN/IMEI` can be altered directly from the keypad using supposedly secret combinations of keystrokes.
    - In other cases, connection to a computer can allow the phone chip to be re-programmed.
- SMS spoofing

Cybercrime Law

- Identifies Standards of acceptable behaviour for information and communication technology (ICT) users.
- Establishes socio-legal sanctions for cybercrime.
- Protects in ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular.
- Protects human rights.
- Enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings) and facilitates cooperation between countries on cybercrime matters.
- Cybercrime law provides rules of conduct and standards of behaviour for:
  - The use of the Internet, computers, and related digital technologies,
  - The actions of the public, government, and private organizations,
  - Rules of evidence and criminal procedure, and other criminal justice matters in cyberspace,
  - Regulation to reduce risk and/or mitigate the harm done to individuals, organizations, and infrastructure should a cybercrime occur.
- Cybercrime law includes `substantive`, `procedural` and `preventive` law.

Chapter 3: Intellectual Property

What's Intellectual Property?

- A legal concept that refers to creations of the mind, such as inventions, literary and artistic works, designs, symbols, and names used in commerce.
- A legal concept that refers to intangible assets (non-physical property), including right of ownership in intellectual property.
- Examples: `patents`, `domain names`, `industrial design`, `confidential information`, `inventions`, `moral rights`, `database rights`, `works of authorship`, `service marks`, `logos`, `trademarks`, `design rights`, `business or trade names`, `commercial secrets`, and `computer software`.

What's Intellectual Property rights?

- Any and all rights associated with intangible assets owned by a person or company and protected against use without consent.

Types of Intellectual Property Rights

- Intellectual property rights include patents, trademarks, copyrights, and trade secrets.
- Owners of intellectual property frequently use more than one of these types of intellectual property law to protect the same intangible assets.
- **Patents**:
  - Exclusive right given to owners to `produce`, `use`, and `sell` an invention.
  - Protects inventions from use by others and gives exclusive rights to one or more inventors.
  - Patents generally expire after a given period usually 20 years.
  - An invention to be patented should be:

        - `Novel` : No technology like it has yet been produced.
        - `Useful` : The invention provides a clear and reasonably accessible benefit to the user.
        - `Non-obvious` : The invention must have a component of innovation and can't be the obvious next step in the development of an existing technology.
        - `Patentable subject matter` : Different countries have different criteria for what can and cannot be patented.
    - Types:
        - `Design patents` : protection for aesthetics of a device or invention (product's shape, emojis, fonts, or any other distinct visual traits).
        - `Plant patents` : safeguards for new varieties of plants.
        - `Utility patents` :
            - Protection for a product that serves a practical purpose and is useful.
            - Examples: `vehicle safety systems` , `software` , and `pharmaceuticals` .
            - The first, and is still the largest, area of patent law.
    - However, patents can be difficult to obtain and the application process can drag out considerably.
- **Copyrights**:
    - Protects the rights of the original creator of original works of intellectual property.
    - Must be tangible.
    - Once someone creates an original work of authorship (OWA), the author automatically owns the copyright.
    - In contrast to a patent, which protects the idea or concept of an invention, copyright protects the specific expression of that idea.
    - It gives the owner the exclusive right to copy, modify, and distribute or sell those copies or modifications of the property to the public.
    - It is automatically obtained by the creation of the original work unlike with patents, there's no need to go through an application process.
    - It is usually applicable for the duration of the copyright owner's life plus 50 years, or for 75 years from publication in the case where the software was created by the employee of a company.
- **Trademarks**:
    - A `symbol` , `phrase` , `name` , or other type of expression used to distinguish a particular product or brand.
    - Names of brands or products are often marked as trademarks using a trademark symbol: ™ for unregistered trademarks, and ® for registered ones.
    - Trademarks protect `logos` , `sounds` , `words` , `colour` , or `symbols` used by a company to distinguish its service or product.
    - Although patents protect one product, trademarks may cover a group of products.

How to protect software intellectual property?

- Software is safeguarded under `copyright` , `trade secret` , and potentially `patent laws` , providing comprehensive protection against unauthorized use or infringement.
- **Preparation Before Release**:

    - Consult a legal team to understand and secure your rights.
    - File patents, register trademarks, and use non-disclosure agreements with employees and contractors.
    - Follow strong data security practices to safeguard your work.
- **Post-Release Protection**: implement a robust licensing management system to control usage and prevent unauthorized distribution.

License Management Systems

- Help protect intellectual property of software by issuing licenses to users that allow them to use the software only in an authorized manner.
- Each license helps control the use of the software so every use complies with the contract.
- Allows the vendor to track how the licenses that have been purchased by each client are being used.

How to protect software IP with License Management?

- A license authorizes a customer to use product legally.
- A software license is both the contract and the key:
    - As a `contract`, it constitutes a software intellectual property agreement between the vendor and the user as to how the software will be used.
    - As a `key`, it gives the user access to the software and allows them to use it according to the terms of the software intellectual property agreement.
- `License keys` are a kind of code that enables the program to work according to the software intellectual property agreement.

Models of Software License Intellectual Property Protection

- **Licensing hardware (Dongles or USB keys)**:
    - Type of license application requires the user to plug a physical electronic device into the computer on which they intend to use the software.
    - The code for the license is programmed into the hardware key and enables the device to access the software.
    - Advantage: very secure and doesn't require reliance on the cloud or Internet access to activate the license.
    - Disadvantage: relatively rigid and non-customizable, and transferring the license requires the transfer of a physical object.
- **Software node locked, host locked, or single-use licenses**:
    - Same as the above but the code to activate the software is delivered via software that is installed or downloaded to a specific device.
    - Advantages: no physical device is required.
    - Disadvantage: the license only applies to a single computer or device, so it can be transferred.
- **Floating, network or concurrent licenses**:
    - License code that is installed or downloaded to the device that can be shared among users on a network.

    - This model is an excellent solution if a company is trying to figure out how to protect intellectual property online.
    - It can be especially cost-effective if a customer needs multiple users or devices to access the software, but not all at once.
    - How it works:
        - The user who needs to access it sends a request for access to a central license server, and the server provides the license based on availability.
        - When the user is done using the software, the license is “returned” to the central server and can then be transferred to a different user.
- **Named user, per-seat, or single-seat licenses**:
    - A license that can only be activated by a particular user who signs in with specific credentials.
    - It is useful if a company knows that only specific employees will need to access this software.
- **License borrowing or offline licenses**:
    - This model allows a user to download a software license and use it without needing to connect to the central license server each time they log in, and then “return” the license once they no longer need to use it offline.
    - Useful for employees who are on the road or in the field and won’t have reliable Internet access.
    - It has the disadvantage of being expensive, since the company will have to pay for the license for the full duration of the period it’s been downloaded to the device.
- **Hybrid Models**: a range or combination of different types of software licenses to best suit the needs of their clients.

Trade Secrets

- `Processes`, `recipes`, `tools`, `mechanisms`, or `formulae` that are not publicly available and are kept secret by its owner to maintain/gain an edge/competitiv advantage over their competitors.
- Company’s intellectual property that isn’t public, has economic value and carries info.
- Trade secrets can be protected by law as long as the owner makes reasonable effort to keep it a secret and no one else has discovered it independently.
- It’s illegal for someone to spy on your company and steal a trade secret, but if they figure it out by reverse engineering or by developing it themselves, it’s fair game.
- Not avaliable for the public.
- Involves information that’s `business`, `financial`, `technical`, `economical`, `scientifical`, and `engineering`.

Challenges of Intellectual Property

- Copyright infringement:
    i. With the widespread availability of digital content, it has become much easier for people to copy and share copyrighted works without permission.

ii. The issue of piracy which refers to the unauthorized use, reproduction, or distribution of copyrighted works is another challenge.
iii. The issue of jurisdiction, with the global nature of the internet, can be difficult
iv. The impact of open-source software on intellectual property

- To address these challenges, several legal and technological solutions can be employed:
  - Governments strengthen intellectual property laws and improve enforcement.
  - Companies can also use digital rights management technologies to protect their intellectual property,
  - Companies have to also explore alternative business models that rely less on traditional intellectual property rights.
  - All stakeholders need to work together address these challenges and ensure that intellectual property is protected in a way that benefits both creators and consumers alike.

Summary

- The digital era presents challenges for intellectual property (IP) protection, including unauthorized copying, online piracy, and jurisdictional variations in enforcement. Emerging technologies like AI and blockchain demand continuous updates to IP laws.

- **Challenges**:
  - Ease of Replication: digital content is easily copied and shared, reducing market exclusivity.
  - Online Piracy: impacts creators' revenue by enabling unauthorized access to content.
  - Jurisdictional Variations: laws differ across regions, complicating enforcement.
  - Technological Advances: AI and blockchain require adaptation of laws to safeguard innovation.
- **Opportunities**:
  - Digital Rights Management (DRM): enables access control and content protection.
  - Wider Audience Reach: Digital tools allow creators to monitor use, analyze behavior, and explore new markets.
  - Fair Use Doctrine: Permits limited reproduction of copyrighted work for education, research, and criticism under specific conditions.
- **Digital vs. Intellectual Property Rights**:
  - `Intellectual property rights (IPRs)` protect ideas and creations, fostering innovation and fair competition.
  - `Digital property rights` manage ownership and use of digital assets, supporting licensing, revenue generation, and security.
- **Impact of Technology**:
  - AI, blockchain, and data analytics improve transparency, enforcement, and content monitoring.
  - Technologies like augmented reality and virtual reality pose new challenges to copyright and trademark laws.

- **Best Practices for Safeguarding IP**:
    - Use DRM, watermarks, and encryption.
    - Register copyrights and trademarks.
    - Educate employees on IP compliance.
    - Monitor for unauthorized use and enforce legal actions when necessary.

Chapter 4: Networked Communication

Email and Spam

- The rapid growth of email has led to significant challenges due to spam, which now constitutes the majority of email traffic. Spam is inexpensive, highly scalable, and profitable for advertisers, making it a prevalent issue despite its negative impact on productivity and Internet bandwidth.
- **Key Points**:
    - **Volume and Cost**: spam dominates email traffic because sending bulk messages is over 100 times cheaper than traditional advertising.
    - **Sources of Spam**: email addresses are harvested from websites, chat rooms, viruses, and dictionary attacks.
    - **Spam Networks**: bot herders control networks of infected computers (zombies) to send billions of emails daily.
    - **Countermeasures**: ISPs use spam filters to block suspicious emails, but spammers exploit Internet design flaws to disguise their identities.

Censorship

- The attempt to suppress or regulate public access to material considered offensive or harmful.
- Examining in order to suppress or delete anything considered objectionable.
- It invites a person(institution) who supervises conduct and morals an official(institution) who examines materials (as publications or films) for objectionable matter.
- `Internet censorship` is the legal control or suppression of what can be accessed, published, or viewed on the Internet.

What could we censor?

- `Parental` (authority over their children) -> Pornographic material.
- `Employer` (authority over their employees in the workplace) -> Games.
- `Government` (authority over a country) -> Violent materials.
- `International` (authority over the international community) -> Terrorist Newsgroups.

Why Censor?

- `Parents` : seek educational benefits for children but worry about exposure to inappropriate content like adult material.
- `Employers` : concerned about reduced productivity and corporate liability due to personal internet use and access to offensive material during work hours.

- `Pressure Groups` : advocate against offensive web content like pornography, weapon sales, and hate campaigns, pushing for their removal.
- `Legal` : laws in various countries regulate online content, requiring compliance with both local and target audience country laws.

Censorship Strategies

- Metadata is often used to automatically determine whether a site should be blocked or not.
- It is also possible for sites to be added to lists of unacceptable or acceptable sites.
- **Blocking Software**:
  - The software contains list of “objectionable” or “good” sites to which it doesn’t or does allow the web browser access.
  - Example: `Surfwatch` and `Netnanny` .
- **Ratings**:
  - Users can set their browsers to block access to sites using either the `RSAC` or `PICS` rating categories.
  - Requirements:
    - `Syntax for defining labels` : different aspects of the site to be measured like `levels of language` , `nudity` , `sex` and `violence` .
    - `Syntax for labeling content` : rating classification for each labels before giving its value.
    - `Method of retrieving labels` : storing and retrieving labels.
- **Service Providers**:
  - Done by `Internet Service Providers (ISPs)` .
  - Each user is then given a corresponding level of “access authority”.
  - The ISP can then run the appropriate software to block access to sites based on the user’s access level.
  - This can be based on block lists or site ratings.
- **Browsers and search engines**:
  - Incorporate censorship features, such as password systems to control access at different user levels.
  - Additionally, some search engines use user feedback to determine whether certain sites should be removed from their index.
- **Social Methods**:
  - Emphasize individual responsibility, whether by employers, parents, or website designers, to implement effective strategies.
  - Users must be educated on the moral and ethical implications of data access and control, fostering awareness of the broader issues involved.
  - Education plays a critical role in promoting responsible actions and must be addressed from a global perspective to ensure a comprehensive understanding.

Censorship and Controversy

- Who has the power to decide which sites are “good” or “bad”? Who is in control the one who rates or the one using the ratings?

    - Closed group
    - Community
    - Individual users
    - Imposed
- **Direct censorship**:
    - `Government monopolization` : government controls and suppress the flow of information.
    - `Prepublication review` : government keeps informations and materials from the general public and block publication of material deemed injurious to the reputations of their rulers.
    - `Licensing and registration` : limiting and controlling media with limited bandwidth.
- **Self censorship**:
    - Group deciding for itself not to publish material.
    - Publishers have adopted ratings systems as a way of helping people decide if they (or their children) should access particular offerings.

Freedom of Expression

- It ensures the right to share thoughts, criticize injustices, and advocate for change without state interference.
- However, concerns arise over harmful or unproductive content, especially for children, employees, and society at large.
- Institutions like the Electronic Frontier Foundation advocate for protecting this freedom, but balancing it with responsible use and regulation remains a challenge, particularly in contexts like education, workplaces, and public discourse.

Trust on the Internet

- **Trust as a Key Factor**:
    - Trust is essential socially, economically, and politically.
    - It connects to personal happiness, well-being, problem-solving, and social cohesion.
- **Challenges to Trust on the Internet**:
    - The Internet was not designed with trust or security in mind.
    - Anonymity and decentralized governance make trust difficult.
    - Privacy breaches, cyberattacks, and misinformation undermine trust.
    - Lack of a central authority complicates regulation and oversight.
- **Impact of Decentralization**:
    - Anyone can participate and host content, fostering inclusivity.
    - Governance becomes challenging due to the Internet's global and decentralized nature.
- **Ethical Issues and the Social Contract**:
    - An implicit social contract governs online behavior (e.g., avoiding all-caps in emails).
    - These unwritten rules emerge from collective interactions and relationships.
    - Understanding this social contract can help address ethical concerns.

Social Contract Principles (Based on Hobbes)

- **Equality in Nature**:
    - All individuals possess equal physical and mental abilities.

    - Natural rights arise from this equality, meaning no one is born with inherent authority over another.
    - People band together to increase their collective power, forming societies to preserve and manage their lives.
- **Conflict and Cooperation**:
    - Competition arises when two people desire the same goal or resource, leading to conflict.
    - To counter this, individuals unite their strengths, but some may act preemptively to avoid future attacks.
    - This creates a “state of nature,” where every individual is in a constant struggle to achieve their ends.
- **State of Nature**:
    - In the absence of a common authority, individuals exist in a state of perpetual war, with “every man against every man.”
    - Hobbes argues that such a state is unsustainable, leading to three choices:
        - Remain in the state of nature.
        - Form a limited government (which he argues is unstable).
        - Establish a commonwealth under a sovereign with unlimited authority.
- **The Role of a Sovereign**:
    - Hobbes concludes that only a sovereign with absolute power can maintain order and prevent the chaos of the state of nature.
    - Even tyranny is preferable to the anarchy and perpetual conflict of a state of war.
- **Relevance to the Internet**:
    - The Internet mirrors Hobbes’ state of nature, as it lacks a central authority.
    - Its decentralized structure leads to challenges in governance and accountability.
    - Hobbes’ theory suggests that absolute authority might bring order, but this perspective is often criticized as overly pessimistic.

Future Trends in Online Trust

- **Strengthening Trust**:
    - Trust in online systems may improve as technology evolves and regulatory frameworks mature.
    - Younger generations and tech-dependent populations will lead in embracing and adapting to these changes.
    - Enhanced systems, combined with industry and policy reforms, will contribute to building trust.
- **Fluid Nature of Trust**:
    - Trust will become more situational, varying depending on the context and relationships involved.
    - It will no longer be binary but distributed across different levels based on circumstances.
    - Sacrifices tied to trust such as privacy trade offs may become normalized as a “side effect of progress.”
- **Challenges to Trust**:
    - Blockchain is often seen as a potential tool to enhance trust, but its real-world impact might be less transformative than expected.

    - For many, the current state of trust in online systems is unlikely to change significantly in the near future.
    - Concerns about security and privacy breaches, coupled with criminal exploits and powerful corporate or governmental interests, will continue to undermine trust.
    - The perception that “anything can be hacked” will persist, making it difficult to rebuild confidence.
- **Adaptation and Resignation**:
    - As convenience dominates, users may become increasingly resigned to risks, feeling they have little choice but to comply and hope for the best.
    - Despite technological advances, trust will remain a complex and evolving issue, shaped by both progress and persistent vulnerabilities.

Broader Exploitation of Trust

- **Building Trust through Technology and Personal Control**:
    - Distributed privacy, personal software agents, and greater individual control over personal data could enhance trust.
    - Blockchain and similar technologies may play a role, not just through encryption but by enabling decentralized transactions.
    - While corporations will enter these new fields, they won’t fully dominate them, akin to how mobile phone minutes became a pseudo-currency in Africa.
- **Trust and Convenience vs. Security**:
    - Despite rising data breaches, people continue to rely on their devices due to convenience.
    - Trust remains stable until significant breaches, such as account hacks, trigger temporary concern.
    - Ironically, even as breaches increase, users continue sharing sensitive data like biometrics and locations.
- **Generational Shifts in Trust**:
    - Younger “social machine natives” will inherently trust their interconnected environments, unlike older generations who may remain skeptical.
    - However, as people learn more about the underlying technologies, they may trust less due to increased awareness of risks.
- **Healthy Skepticism and the Role of Regulation**:
    - A slight reduction in trust might lead to healthier, more cautious online behavior.
    - Trust in online interactions could improve if technologies are designed with safeguards and if regulations address surveillance capitalism and data abuse effectively.
- **Convenience at the Cost of Agency**:
    - The trade-off between convenience and control over personal data is reaching a tipping point.
    - The growing complexity and opacity of digital services erode individual agency, creating a “Faustian bargain” many users don’t consciously make.
- **Promoting Positive Outcomes**:
    - Instead of focusing on fears, stakeholders—technologists, governments, media, and educators should highlight opportunities and benefits.

    - By addressing risks and exploring what can go right, trust can be nurtured alongside innovation.
- **Implicit and Unconscious Trust**:
    - Most people trust online systems unconsciously until a breach forces them to reconsider.
    - Technologies like HTTPS and recognition systems are essential to mitigate risks and guide users toward better practices.
- **The Need for Accountability**:
    - Expanded “public defenders” for online systems could build trust, providing clear accountability, addressing failures, and promoting transparency.
    - Public reporting of cybercrimes and errors, akin to crime or airline data, could foster a culture of trust and improvement.
- **Resignation to Risks**:
    - People will continue to prioritize convenience over trust, navigating the risks as part of daily life, much like driving despite traffic and accidents.
    - While users may grumble about security issues, online interactions will remain indispensable, with trust implicitly guiding their behaviori.

Internet Addiction

- An overwhelming need to use the internet to the detriment of one’s health and daily functioning.
- Otherwise known as `problematic internet use` or `compulsive internet use`, is a behavioural disorder characterized by an excessive or poorly controlled preoccupation, urges, or behaviours regarding internet use that lead to impairment or distress.
- **Symptoms**:
    - Euphoria when online
    - Fatigue
    - Sleep problems
    - Muscle aches and pains resulting from inactivity
    - Dry eyes or other eye problems
    - Digestive problems
    - Unintended weight loss or weight gain
    - Preoccupation with the internet
    - Excessive time online
    - Withdrawal symptoms
    - Problems at work or school
    - Lying about internet use
    - Neglecting personal hygiene
    - Withdrawal from face-to-face social interactions
- **Causes**: various factors that contribute to the development and persistence of compulsive internet use.
    - Genetics: `Autism Spectrum Disorder (ASD)`, `Bipolar Disorder (BPD)`, `Schizophrenia (SCZ)`, and `Attention Deficit Hyperactivity Disorder (ADHD)`.
    - Psychological factors: `stress`, `anxiety`, `depression`, or `low self-esteem`.
    - Environment influences
    - Peer pressure

    - Instant gratification

Why is the Internet Addictive?

- The internet combines psychological, social, and technological factors to create a highly engaging experience.
- It provides instant gratification and constant stimuli, triggering dopamine release and reinforcing usage.
- Social platforms offer connection, validation, and engagement, appealing to those seeking community.
- Features like infinite scrolling, personalized content, and push notifications are designed to encourage prolonged use.

Types of Internet Addiction

- Computer or gaming addiction
- Compulsive information seeking
- Cybersex addiction
- Net compulsions
- Cyber (online) relationship addiction

Effects of Internet Addiction

- Social isolation
- Negative online experiences
- Health risks
- Sleep disorders
- Poor academic performance
- Impaired relationships

Treatments for Internet Addiction

- Psychotherapy
- Family therapy
- Medication
- Lifestyle changes
- Digital detox programs

Overcoming Internet Addiction

- Involves a well-structured strategy that integrates self-awareness, behavior modification, and support systems, often encapsulated in 12 key steps.
- **Includes**:
    - Acknowledging the problem
    - Setting specific goals
    - Limits for internet use
    - Creating a balanced daily routine
    - Creating a balanced offline activities11.Practicing mindfulness

- Identifying triggers
- Using productivity tools
- Seeking professional help
- Building a support network
- Creating technology-free zone