COMPUTING ETHICS

Foundations of Ethics and Computing

- A foundational challenge in computing ethics is that the terms ethics, morals, and law are frequently used interchangeably in everyday conversation.
- As computing professionals, we require precise definitions.
- Decisions in software design, data governance, and system deployment rest on clear distinctions between what is legal, what is moral, and what is ethical.

Ethics

- Ethics is the branch of philosophy concerned with what is right and wrong, good and bad, and how individuals and groups ought to behave.
- It is a systematic, rational discipline that seeks to justify moral beliefs through principles, arguments, and reasoning. In computing, ethics operates at multiple levels:
- **Individual level**: How a software engineer personally decides whether to include tracking code in an app.
- **Organizational level:** How a company establishes policies around user data collection.
- **Societal level**: How governments and professional bodies regulate AI systems.
- The key distinguishing feature of ethics is its emphasis on reasoned justification.
- It is not enough to feel that something is wrong; ethics demands that you be able to explain why, using coherent and defensible principles.

Morals

- Morals refer to personal or culturally-held beliefs about right and wrong. They are typically absorbed through upbringing, religion, culture, and experience rather than derived through formal philosophical reasoning.
- While ethics asks "what should I do and why?", morals reflect "what do I believe is right?"
- In a computing context, moral beliefs vary widely. One developer may morally object to building surveillance tools even if they are legal; another may regard it as simply a job. This variation creates tensions that ethical frameworks help us navigate.
- Note the distinction: a person can act in accordance with their morals but still act unethically —
- if their moral beliefs are themselves unjustifiable under scrutiny. Ethics provides the tools to examine and critique moral positions.

Law

- Law comprises rules formally enacted and enforced by a governing body. Laws set a minimum standard for behavior and carry enforceable consequences.
- Crucially, law and ethics do not always align. Consider these scenarios:
  - Scenario 1 — Collecting user data with buried consent in Terms and Conditions: Legal? Yes, in many jurisdictions. Ethical? Debatable — users lack meaningful informed consent.
  - Scenario 2 — A whistleblower leaking evidence of corporate wrongdoing: Legal? Often, no breach of contract or confidentiality. Ethical? Many argue yes — acting to prevent harm to the public.
  - Scenario 3 — Selling legally acquired user data to third parties: Legal? Yes, where no law prohibits it. Ethical? No — violates user trust and the reasonable expectation of privacy.

TRADITIONAL ETHICAL THEORIES

Consequentialism (Utilitarianism)

Core Principle

- Utilitarian ethical theories are based on one's ability to predict the consequences of an action. To a utilitarian, the choice that yields the greatest benefit to the most people is the one that is ethically correct.

- An action is morally right if it produces the greatest good for the greatest number of people.

- The rightness of an action is judged entirely by its outcomes and its consequences.

- Associated most strongly with philosophers Jeremy Bentham (1748–1832) and John Stuart Mill (1806–1873).

Key Concepts

- **Utility:**
  - The measure of benefit, happiness, or welfare produced by an action.
- **Act Utilitarianism:**
  - Each individual act is evaluated based on its specific consequences in the particular situation.
  - a person performs the acts that benefit the most people, regardless of personal feelings or societal constraints such as laws.
- **Rule Utilitarianism:**
  - We follow rules that, in general, tend to produce the greatest good
  - for example, "always obtain informed consent before collecting personal data“. Even if in a specific case, breaking the rule might produce more utility.
  - A rule utilitarian seeks to benefit the most people but through the fairest and most just means available.

Application to Computing

- A social media company may argue that personalized content recommendations, even if they require extensive personal data, maximize user engagement and therefore utility.

- A consequentialist analysis would need to ask more rigorously: does the aggregate benefit (better content discovery, social connection, commercial opportunity) genuinely outweigh the harms (privacy erosion, algorithmic manipulation, addiction, mental health effects on vulnerable users)?

Critique

Strengths of Consequentialism

- Practical and outcome-focused — it asks us to look at real-world impacts.
- Flexible — it can be applied to technologies that did not exist when it was developed.
- Widely used in policy analysis, cost-benefit analysis, and risk assessment frameworks.
- Intuitive — most people instinctively think consequences matter morally.

Weaknesses of Consequentialism

- Can justify harm to minorities if the majority benefits — the aggregate good can mask individual injustice.
- Difficult to accurately predict all consequences of complex technical systems.
- Can neglect individual rights and duties — the ends do not always justify the means.
- Who counts in the utility calculation? Future generations? Animals? Those outside a jurisdiction?

Deontological Ethics (Duty-Based Ethics)

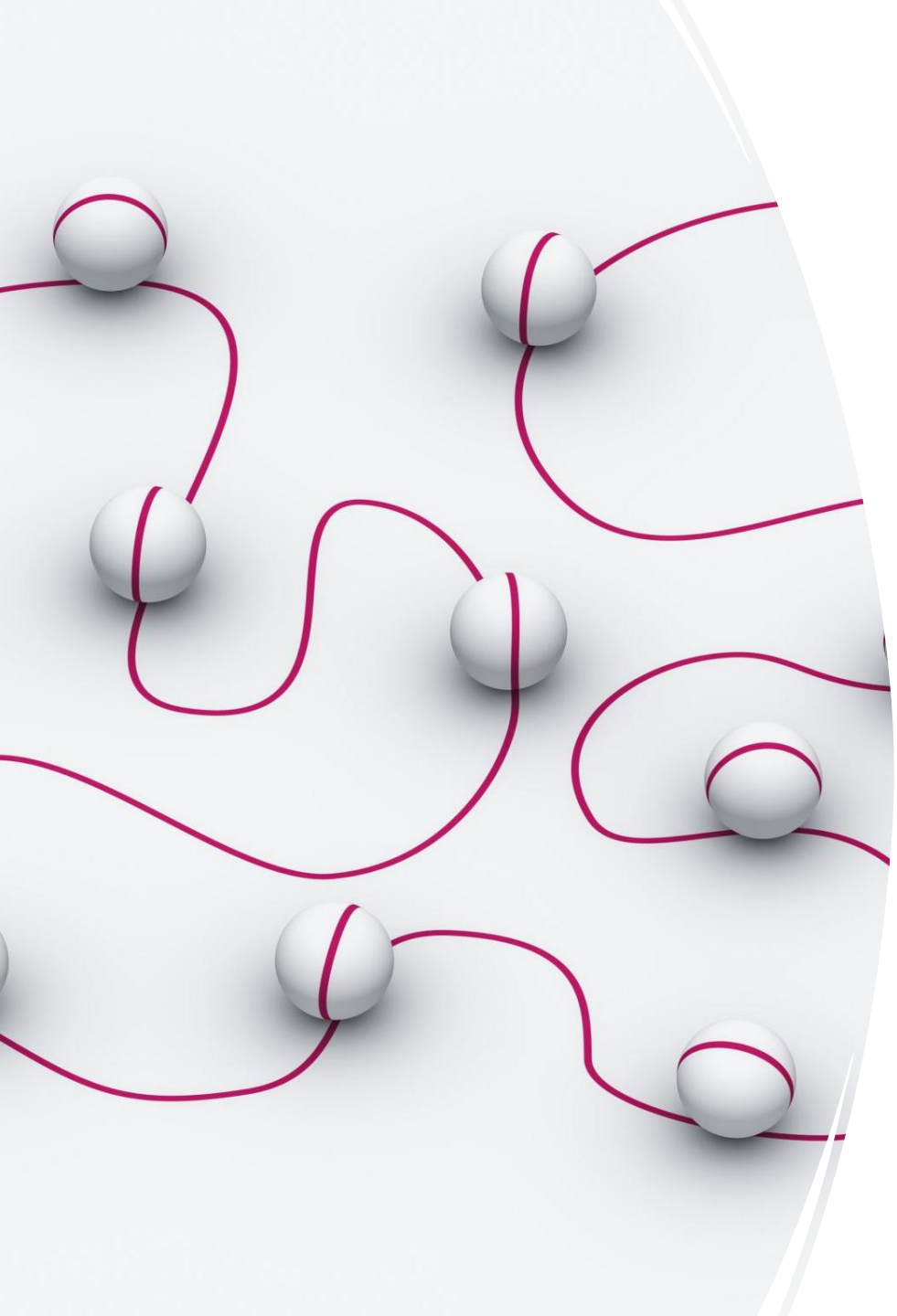
Core Principle

- The deontological class of ethical theories holds that people should adhere to their obligations and duties when making decisions in ethical contexts.
- Actions are right or wrong in themselves, regardless of their consequences.
- Our duty is to follow moral rules. Most associated with the German philosopher Immanuel Kant (1724–1804) and his Categorical Imperative
- This means that a person will fulfill their obligations to another individual or society because upholding one's duty is considered ethically correct.

Advocates

if every developer did this, what would the world look like? If every app used deceptive dark patterns, the entire digital ecosystem would become untrustworthy.

Users must not be reduced to data points to be exploited for commercial gain. Every person interacting with a system has inherent dignity that must be respected.



Application to Computing

- A deontological approach argues that deceiving users regardless of the commercial benefit is inherently wrong, because deception treats people as means rather than ends.
    - Eg: Dark patterns in user designs that make subscription cancellation deliberately confusing, hiding unsubscribe buttons, using misleading language on buttons violates the duty to treat users as rational autonomous agents
    - In case of a Data Breach: A deontological approach would hold that a company has a duty to disclose a data breach to affected users, even if the disclosure causes reputational harm and no law yet requires it, because users have a right to know about violations of their personal information.

Critique

Strengths of Deontology

- Protects individual rights even when they conflict with majority interests.
- Provides clear duties that do not require complex consequence calculations.
- Reflects widely-held moral intuitions about human dignity and respect.
- Provides a foundation for human rights frameworks.

Weaknesses of Deontology

- Can produce counterintuitive results — following a rule even when breaking it would clearly prevent harm.
- Different duties can conflict with each other (e.g., duty to protect users vs. duty to comply with government data requests).
- Does not easily accommodate context — all situations are treated by the same rules regardless of specifics.

Virtue Ethics

Core Principle

- Rather than focusing on rules or consequences, virtue ethics asks: what kind of person should I be?
- It centres on cultivating good character traits (virtues) that guide consistent ethical behaviour across situations.
- Key virtues include honesty, integrity, courage, fairness, compassion, and practical wisdom (phronesis).
- Where consequentialism asks "what will produce the best outcome?" and deontology asks "what is my duty?", virtue ethics asks "what would a person of good character do in this situation?"

Application to Computing

- **Integrity:**
  - A developer who discovers a security flaw discloses it honestly rather than ignoring it to avoid blame or embarrassment.
- **Honesty:**
  - A data scientist accurately reports the limitations and uncertainty of their model rather than overselling accuracy to clients or management.
- **Prudence:**
  - A systems architect proactively considers failure modes, edge cases, and potential misuse before deployment rather than after something goes wrong.
- **Courage:**
  - An engineer speaks out against a product feature they believe will harm users, even when facing organisational pressure to comply.
- **Fairness:**
  - A product manager ensures that testing and quality assurance include diverse user groups, not just the majority demographic.

Critique

Strengths of Virtue Ethics

- Focuses on the agent rather than isolated acts — builds professional character.
- Flexible and context-sensitive — wisdom guides application to specific situations.
- Aligns naturally with professional culture and mentorship.
- Covers situations where no specific rule exists.

Weaknesses of Virtue Ethics

- Less action-guiding in specific dilemmas — "be courageous" does not tell you exactly what to do.
- Virtues can conflict with each other (honesty and compassion may pull in different directions).
- Culturally variable — virtues are not universally agreed upon.

PROFESSIONAL RESPONSIBILITY IN COMPUTING

Professional Responsibility

- A profession is distinguished from a mere occupation by three key features:
  - A specialized body of knowledge,
  - Formal training and credentialing,
  - An obligation to serve the public good rather than solely the interests of the employer or client.

Four dimensions of Professional Responsibility

Professional responsibility in IT encompasses four dimensions:

1. Technical responsibility: Ensuring systems are correct, reliable, secure, and performant.

2. Ethical responsibility: Ensuring systems are just, transparent, fair, and do not cause undue harm.

3. Social responsibility: Considering the broader societal effects of the systems we build and deploy.

4. Legal responsibility: Compliance with applicable laws and regulations in all relevant jurisdictions.

Codes of Conduct

ACM Code of Ethics and Professional Conduct (2018)

- The Association for Computing Machinery Code is structured around four sets of principles:

1. **PRINCIPLE SET 1 — General Ethical Principles:**
    - Contribute to society and human wellbeing; ensure that computing benefits society.
    - Avoid harm — acknowledge and mitigate unintended harms that arise from systems.
    - Be honest and trustworthy in all professional interactions.
    - Be fair and take action not to discriminate.
    - Respect the work required to produce new ideas, inventions, creative works, and artefacts.
    - Respect privacy.
    - Honour confidentiality.

PRINCIPLE SET 2 : Professional Responsibilities:

- Strive to achieve high quality in processes and products.
- Maintain high standards of professional competence, conduct, and ethical practice.
- Know and respect existing rules pertaining to professional work.
- Accept and provide appropriate professional review.
- Give comprehensive and thorough evaluations of computer systems and their impacts.
- Perform work only in areas of competence.
- Foster public awareness and understanding of computing.
- Access computing and communication resources only when authorised to do so.
- Design and implement systems that are robustly and usably secure.

PRINCIPLE SET 3 :Professional Leadership Principles:

- Ensure that the public good is the central concern during all professional computing work.
- Articulate, encourage acceptance of, and evaluate fulfilment of social responsibilities by members of the organisation.
- Manage personnel and resources to enhance the quality of working life.
- Articulate, apply, and support policies and processes that reflect the code's principles.
- Create opportunities for members of the organisation to grow as professionals.
- Use care when modifying or retiring systems.
- Recognise and take special care of systems that become integrated into the infrastructure of society.

PRINCIPLE SET 4 : Compliance:

- Uphold, promote, and respect the principles of this Code.
- Treat violations of this Code as inconsistent with membership of the ACM

BCS Code of Conduct (UK)

- The British Computer Society Code requires members to act with integrity across four domains:
  - **Public Interest:**
    - Have due regard for public health, privacy, security, and wellbeing of others and the environment. Have due regard for the legitimate rights of third parties.
  - **Professional Competence and Integrity:**
    - Only undertake work that you are competent to perform. Act with integrity, be honest and fair to your clients, employers, and colleagues. Accept professional responsibility for your work.

Cont’d

Duty to Relevant Authority:

- Act with due skill, care, and diligence in carrying out your employer's or client's legitimate instructions. Avoid conflicts of interest between your work and personal interests.

Duty to the Profession:

- Seek to improve professional standards. Conduct yourself with integrity in all professional relationships. Support efforts to advance understanding of IT.

Ethical rules for computer users

- Do not use computers to harm other users.
- Do not use computers to steal others' information.
- Do not access files without the permission of the owner.
- Do not copy copyrighted software without the author's permission.
- Always respect copyright laws and policies.
- Respect the privacy of others, just as you expect the same from others.

Cont’d

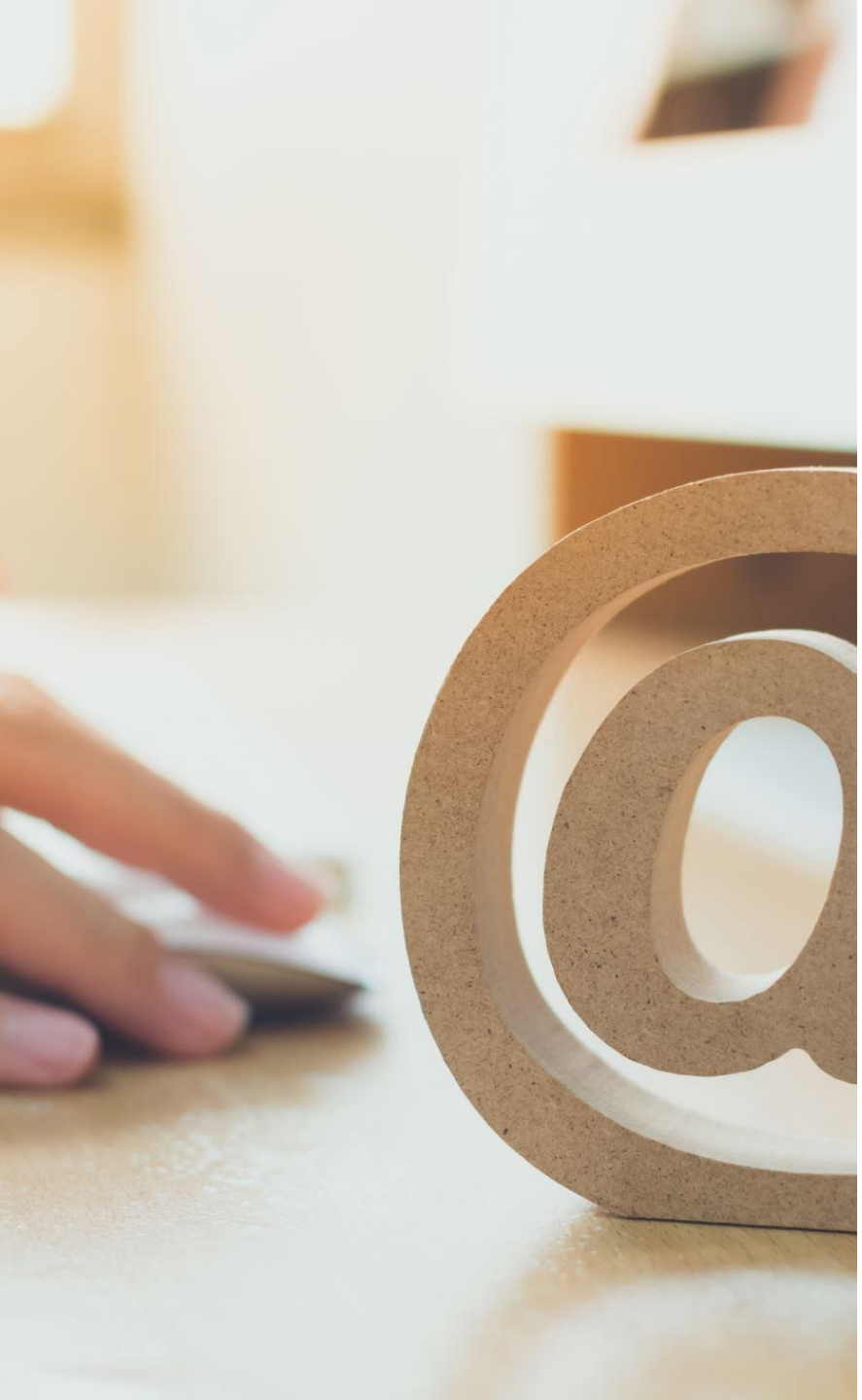
- Do not use another user’s computer resources without their permission.
- Use the Internet ethically.
- Complain about illegal communication and activities, if found, to Internet service Providers and local law enforcement authorities.
- Users are responsible for safeguarding their User Id and Passwords. They should not write them on paper or anywhere else for remembrance.
- Users should not intentionally use the computers to retrieve or modify the information of others, which may include password information, files, etc.

Formal codes of conduct

- These are codes of conduct as outlined and enforced by the organization in their policies, which all personnel within the organization have to agree to abide by.
- These policies are written down and signed, and include:
  - ACCEPTABLE USE POLICY
  - INTERNET ACCESS POLICY

Acceptable use policy

- Employees within an organization may have access to sensitive *data* about their customers and clients. If so, they must treat this data with respect and in accordance with the law. An acceptable use policy sets out what is and is not acceptable and clearly explains the use of electronic devices to establish ethical and lawful behavior.
- For instance, it may specify:
  - employees are not allowed to copy personal information from clients onto a removable storage media device and take it out of the office
  - data needs to be *encrypted* before it is sent via email
  - Paper copies of sensitive data must be destroyed once they are no longer needed



Internet access policy

- An internet access policy provides employees with rules and guidelines about the appropriate use of the internet while in the workplace.

It may specify:

- Employees are expected to use the internet responsibly and productively
- Internet access is limited to job-related activities only, and personal use is not permitted
- The organisation reserves the right to monitor internet traffic and monitor and access data that is composed, sent, or received through its online connections
- E-mails sent via the company email system should not contain content that is classed as offensive or include vulgar language and images, or can be interpreted as bullying to another party

Computing Dilemmas

Common Categories

- Computing professionals regularly encounter ethical dilemmas across several recurring domains. It is useful to recognize the categories:
- **Privacy and Surveillance**:
  - Location tracking in apps; employer monitoring of remote workers; facial recognition in public spaces without consent.
- **Intellectual Property:**
  - Open source versus proprietary software; reverse engineering for security research; ownership of AI-generated creative works.
- **Algorithmic Bias**:
  - Discriminatory credit scoring; biased hiring algorithms; predictive policing systems that concentrate enforcement on minority communities.

Cont’d

- **Security and Disclosure:**
  - Responsible vulnerability disclosure; government requests for security backdoors; ransomware negotiation.
- **Artificial Intelligence:**
  - Autonomous, generative AI deepfakes enabling political misinformation.
- **Digital Divide:**
  - Unequal access to digital services; automated systems that disadvantage citizens with limited digital literacy.
- **Environmental Impact:**
  - Energy consumption of data centers and blockchain mining; accelerating e-waste from device obsolescence cycles.

Resolving Computing Dilemmas

- **Step 1**
  - Identify and Clearly Define the Ethical Issue: What exactly is the dilemma? Resist the temptation to act before you have clearly articulated what the problem is. Who are all the stakeholders — directly and indirectly affected?
- **Step 2**
  - Gather Relevant Facts: What do you know with confidence? What are you assuming? What critical information is missing or uncertain? Ethical analysis based on incomplete facts produces unreliable conclusions.
- **Step 3**
  - Identify Stakeholders and Their Interests: Who is affected by this decision, and how? What are their rights? What duties do you owe them? What are their legitimate expectations? Include those who are absent from the room — end users, marginalized communities, future generations.

Cont’d

- **Step 4**
  - Identify All Available Options: Do not assume the dilemma is binary. Ethical dilemmas are often framed as "do X or do Y" when creative alternatives exist that reduce the harm of both options. What is the full range of possible actions?
- **Step 5**
  - Make a Decision and Test It: Would you be comfortable if your decision were reported publicly — in a newspaper, to your professional body, to the people most affected? Does it accord with your professional code of conduct? Could you explain and defend it to all the stakeholders you identified?
- **`Step 6**
  - Act, Document, and Reflect: Implement the decision. Document your reasoning at the time — not retrospectively. Subsequently, evaluate the outcomes: were the consequences you anticipated what actually occurred? What would you do differently? Ethical reasoning improves through practice and reflection.

Cyber Law and Regulation in Uganda

What Are Cyber Laws?

- **Cyber laws**
  - Also called information and communications technology (ICT) law or internet law
  - Are legal rules that govern the use of computers, networks, digital communications, and electronic data.
  - They define rights, obligations, and offences in cyberspace.
- **Think:**
  - How many of you students use mobile money, social media, or online shopping? Do you know which law protects you when doing so

Introduction

- Cyber laws have evolved as societies have become increasingly dependent on digital technologies.

- Early internet users operated in a largely unregulated environment, but as threats such as cybercrime, data breaches, and online fraud emerged, governments introduced **cyber laws** to regulate conduct and **cybersecurity policies** to safeguard national interests.

Why Cyber Laws Matter

- **Cybercrime growth**
  - Hacking, fraud, and harassment are rising; citizens need legal recourse and certainty about what conduct is criminal.
- **E-commerce expansion**
  - Online contracts, digital payments, and electronic receipts need legal validity to support commerce and consumer protection.
- **Data exploitation**
  - Personal data collected by apps and platforms must be regulated to prevent misuse and protect citizen rights.

Cont’d

- **National security threats**
  - Communications interception requires legal authorisation and limits to prevent abuse.
- **Digital identity**
  - Electronic signatures and transactions need legal equivalence to paper documents and handwritten signatures.
- **Consumer protection**
  - Citizens transacting digitally must have rights that are enforceable in court against merchants and service providers.

Functions of Cyber Laws

- **Criminalize:**
  - Define and penalize unauthorized access, data theft, fraud, and online harassment, making clear what conduct is illegal and what consequences follow.
- **Validate:**
  - Give legal status to electronic contracts, signatures, and records, enabling digital commerce and e-government to function with legal certainty.
- **Protect:**
  - Regulate how personal data is collected, stored, and shared, safeguarding citizens' privacy and dignity in the digital sphere.

Cont’d

- **Authorize:**
- Define the powers of government and law enforcement in cyberspace, including when and how the state may intercept communications or restrict digital services.
- **Balance:**
- Mediate between individual freedoms expression, privacy, access to information and state interests in security and public order.

Uganda’s Cyber Law Timeline

- Uganda, like many developing economies, experienced rapid digital transformation in the 2000s — e-government, mobile money, online services, and digital banking.
- This growth brought new risks such as cyber fraud, identity theft, and data breaches.
- In response, Uganda developed cyber laws and policy frameworks to safeguard digital transactions, regulate online behavior, and enhance cybersecurity.

Key Legislative and Policy Milestones

- Uganda enacted **three landmark pieces of legislation**:
- **Computer Misuse Act, 2011**
  - Criminalizes unauthorized access, cyber harassment, child pornography, electronic fraud, and computer misuse.
  - Establishes penalties for cybercrime offenses.
- **Electronic Transactions Act, 2011**
  - Provides legal recognition of e-commerce and electronic contracts.
  - Facilitates online services, digital payments, and e-signatures.
- **Electronic Signatures Act, 2011**
  - Establishes a legal framework for secure electronic signatures and certification authorities.
  - Supports authentication in electronic transactions

Recommended Readings

- *Computer Misuse Act, 2011.*
- *Electronic Transactions Act, 2011.*
- *Electronic Signatures Act, 2011.*
- *Data Protection and Privacy Act, 2019.*
- Regulation of Interception of Communications Act (2010)
- Uganda Communications Act (2013)

Q&A