**COMPUTING ETHICS**
**GROUP WORK DISCUSIONS**

## Examining Uganda's Digital Governance Laws: Ethical Implications for Computing Professionals

In today's digital society, computing professionals operate within complex legal and ethical environments shaped by national and international regulations. In Uganda, key laws such as the Computer Misuse Act, the Data Protection and Privacy Act, the Regulation of Interception of Communications Act, the Uganda Communications Act, the Electronic Transactions Act, and the Electronic Signatures Act form the legal backbone of the country's digital ecosystem. However, legality does not automatically equal ethicality. This group assignment requires students to critically examine these Acts not only as legal instruments but as ethical frameworks that influence professional conduct, system design, cybersecurity practices, digital rights, privacy, freedom of expression, surveillance, AI development, and online governance. Students must analyze how these laws shape moral responsibility in computing and evaluate their broader societal implications.

## Instructions to Students

Each group must independently research, find, and download the official, most recent version of their assigned Act from credible sources, such as government websites, official legal repositories, or recognized legal databases.

**Students are expected to:**

- Read the entire Act (not summaries or secondary commentaries only).
- Identify and analyze the specific sections relevant to your allocated focus area.
- Cite specific provisions (sections and clauses) during your discussion and presentation.
- Critically evaluate how the Act influences ethical decision-making in computing practice.

**GROUP ALLOCATION OF REGULATIONS AND LAWS**

## 1. The Computer Misuse Act

These groups must examine how this law addresses cybercrime and online behavior and evaluate the ethical tensions it creates.

**Groups 1, 2, 3**

Focus distribution:

- **Group 1:** Ethical foundations (crime vs freedom of expression, legality vs morality)
    - Analyze the tension between crime and freedom of expression.
    - Examine legality vs morality (Is something ethical simply because it is legal?).
    - Discuss over-criminalization and digital rights.
- **Group 2:** Cybercrime, online harm, and social media ethics
    - Evaluate online harassment, misinformation, and digital harm.
    - Assess the ethical responsibility of users vs. the enforcement powers of the state.
    - Discuss proportionality in punishment.
- **Group 3:** Professional responsibility & ethical dilemmas for IT practitioners
    - Identify ethical dilemmas faced by IT professionals under this Act.
    - Discuss whistleblowing, ethical hacking, and penetration testing boundaries.
    - Examine liability and professional conduct standards.

## 2. The Data Protection and Privacy Act

These groups should focus on privacy, consent, surveillance, and AI governance.

**Groups 4, 5, 6**

Focus distribution:

- **Group 4:** Data protection principles and consent
    - Examine consent, purpose limitation, and data minimization.
    - Analyze ethical data handling in system design.

- **Group 5:** Surveillance vs privacy debate (link to interception and monitoring)
    - Debate monitoring, interception, and employee/user surveillance.
    - Discuss ethical limits of tracking technologies.
- **Group 6:** AI, profiling, automated decision-making, and big data ethics
    - Evaluate profiling, algorithmic bias, and fairness.
    - Discuss transparency, accountability, and big data ethics.

## 3. The Regulation of Interception of Communications Act

These groups should analyze surveillance and the ethics of national security.

**Groups 7, 8**

Focus distribution:

- **Group 7:** National security vs individual freedoms
    - Examine the ethical justification for lawful interception.
    - Evaluate proportionality and necessity.
- **Group 8:** Government monitoring, lawful interception, and proportionality
    - Discuss lawful interception frameworks.
    - Analyze risks of abuse of surveillance power.

## 4. The Uganda Communications Act

These groups should examine media regulation and platform governance.

**Groups 9, 10**

Focus distribution:

- **Group 9:** Regulation of media, content moderation, and digital democracy
    - Evaluate media control, censorship, and content moderation.
    - Discuss impact on democratic participation.
- **Group 10:** Platform power, misinformation, and corporate control of discourse
    - Analyze corporate control of online discourse.

- Examine the ethical responsibility of digital platforms.

## 5. The Electronic Transactions Act

These groups should focus on trust and digital commerce.

**Groups 11, 12**

Focus distribution:

- **Group 11:** E-commerce trust, consumer protection, and fraud prevention
  - Examine fraud prevention, trust-building, and cybersecurity ethics.
  - Discuss user protection in online transactions.
- **Group 12:** Ethical system development and secure digital infrastructure
  - Analyze secure system design.
  - Evaluate professional duty in building resilient digital infrastructure.

## 6. The Electronic Signatures Act

These groups should focus on trust, authentication, and professional implementation.

**Groups 13, 14**

Focus distribution:

- **Group 13:** Authenticity, non-repudiation, and trust in digital systems
  - Examine digital identity, verification, and trust mechanisms.
  - Discuss the ethical importance of secure authentication systems.
- **Group 14:** Professional responsibility in secure implementation & identity management
  - Analyze risks of weak identity management.
  - Evaluate the accountability of developers and system architects.

## NB: What All Groups Must Do

Regardless of allocation, each group is expected to:

1. Explain the key provisions of the assigned Act.
2. Identify the ethical issues arising from the Act.

3. Apply ethical theories.
4. Discuss implications for computing professionals.
5. Provide practical examples or case scenarios.
6. Critically evaluate whether the law adequately balances innovation, security, and human rights.