Data Protection, Privacy and Digital Rights

Personal Data

- Under the Uganda Data Protection and Privacy Act 2019 (DPPA), personal data is defined as any information relating to an identified or identifiable natural person.
- The EU General Data Protection Regulation (GDPR) uses the same formulation.
- An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.
- The practical implication is broad: the law does not require that data identify a person by name. If data can be linked back to an individual through a combination with other available data, it counts as personal data, and the full protections of the law apply.

Categories of Personal Data

- **Direct Identifiers**: Examples: Full name, national ID number, passport number, email address.
- These identify a specific person on their own without requiring any additional data. The connection between the identifier and the individual is immediate and unambiguous.
- **Quasi-Identifiers**: Examples: Date of birth, gender, postcode, employer name, occupation.
- These data points may not identify a person individually, but when combined with each other or with other available data, they can uniquely identify an individual.
- Research has demonstrated that as few as three quasi-identifiers, such as date of birth, gender, and postcode, are sufficient to uniquely identify the majority of individuals in a given population.

Cont’d

- **Online Identifiers**: Examples: IP address, cookie identifier, device identifier, username, browsing fingerprint.
- Increasingly treated as personal data under modern law, even though they do not directly reveal a person's name. An IP address logged by a website operator, combined with internet service provider records, identifies a specific subscriber.
- **Location Data**: Examples: GPS coordinates, home address, workplace address, travel patterns, and routes.
- Location data is among the most sensitive categories of data because it reveals not just where a person is but their patterns of life, such as where they worship, whom they associate with, which medical facilities they visit, and their daily routines.
- **Biometric Data**: Examples: Fingerprints, facial geometry measurements, retinal scan, voice print, gait analysis.
- Uniquely identifies an individual with a high degree of precision. Classified as sensitive personal data requiring enhanced protection under most data protection laws, including the DPPA 2019.

Cont’d

- Examples of Personal Data
  - Name
  - Email address
  - Phone number
  - National ID number
  - Location data
- Sensitive Personal Data-Data requiring higher protection:
  - Health records
  - Biometric data
  - Genetic data
  - Religious beliefs

The Law of Consent

- Permission given by an individual allowing an organization to process their personal data.
- The technology industry has developed sophisticated techniques for manufacturing apparent consent while denying genuine choice.
- Under the DPPA 2019, consent that is relied upon as the lawful basis for data processing must satisfy five cumulative requirements. All five must be present simultaneously
- The absence of any one of them renders the consent invalid.

Conditions for Valid Consent

Cont’d

- **FREELY GIVEN**: What It Means: There must be no coercion, no penalty for refusing or withdrawing consent, and no bundling of consent with the terms of service for an unrelated product. The da
- **SPECIFIC:** What It Means: Consent must be obtained separately for each distinct processing purpose. A single act of consent cannot cover multiple unrelated uses of the data.The subject must have a genuine choice.
- **INFORMED:** What It Means: The data subject must be provided with sufficient information to make a meaningful decision. They must know who is collecting the data, for what purpose or purposes, how long it will be retained, who else will receive it, and what their rights are.

Con’t

- **UNAMBIGUOUS**: What It Means: Consent must be a clear, positive, affirmative act. Passive behaviour
- silence, inaction, continued browsing, or failure to untick a box does not constitute consent
- **WITHDRAWABLE:** What It Means: Withdrawing consent must be as easy as giving it.
- The data subject must be able to withdraw at any time without facing any negative consequence or detriment as a result of the withdrawal.

Data Protection Principles

- Fundamental guidelines governing how personal data should be handled.
- The DPPA 2019 and the GDPR organise their requirements around seven core principles.
- Every specific obligation in data protection law, consent requirements, security measures, data subject rights, retention policies, breach notification duties flows from one or more of these principles.
- A computing professional who genuinely understands these seven principles can reason through almost any data protection question, even in the absence of specific regulatory guidance.

PRINCIPLE 1 — Lawfulness, Fairness, and Transparency

- Data must be processed lawfully: meaning it must have a valid legal basis.

- It must be processed fairly: meaning it must not be processed in ways that are deceptive, unjust, unexpected, or damaging to the data subject.

- It must be transparent: meaning data subjects must be clearly informed about what is being done with their data, by whom, and for what purpose.

PRINCIPLE 2 — Purpose Limitation

- Personal data must be collected for specified, explicit, and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.
- You must state your purposes at the time of collection and be bound by them.

PRINCIPLE 3 — Data Minimisation

- Personal data collected must be adequate, relevant, and limited to what is strictly necessary in relation to the purposes for which it is processed.

- If you do not need data to achieve your stated purpose, you must not collect it.

PRINCIPLE 4 — Accuracy

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

- Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

PRINCIPLE 5 — Storage Limitation

- Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which it is processed.

- When data is no longer needed, it must be deleted or anonymised.

PRINCIPLE 6 — Integrity and Confidentiality (Security)

- Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational security measures.

PRINCIPLE 7 — Accountability

- The data controller is not merely required to comply with all of the above principles
- It must be able to demonstrate compliance.
- Documentation, privacy policies, records of processing activities, staff training, Data Protection Impact Assessments, and audit trails are not bureaucratic overhead.
- They are evidence of compliance.

Privacy

What is Privacy?

- The right of individuals to control their personal information.
- Privacy is recognised as a fundamental human right in international law.
- Article 12 of the Universal Declaration of Human Rights (1948) states that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence.
- Article 17 of the International Covenant on Civil and Political Rights (ICCPR) gives this protection the force of binding international treaty law.
- Uganda ratified the ICCPR in 1995 — these obligations are legally binding on the Ugandan state.

Privacy Rights

- **Autonomy and dignity**: The ability to control one's own narrative, information, and identity is fundamental to what it means to be a free and autonomous person.
- **Freedom of expression**: People who know they are watched alter their behaviour to conform to perceived norms and expectations.
- **Human dignity**

What is Security?

- Measures taken to protect national security, public safety, and prevent crime.
- Reasons:
  - Terrorism and Serious Crime
  - Child Protection
  - Public Health
  - Cybersecurity

Privacy vs Security Debate

- **The "Nothing to Hide" Fallacy:** "if you have nothing to hide, you have nothing to fear" from government surveillance.
- Logically and ethically flawed

- Everyone has private information — medical history, sexual orientation, financial difficulty, political views, family conflicts, personal beliefs — that they have every right to keep from the state, their employer, and other private parties, without being suspected of any wrongdoing.

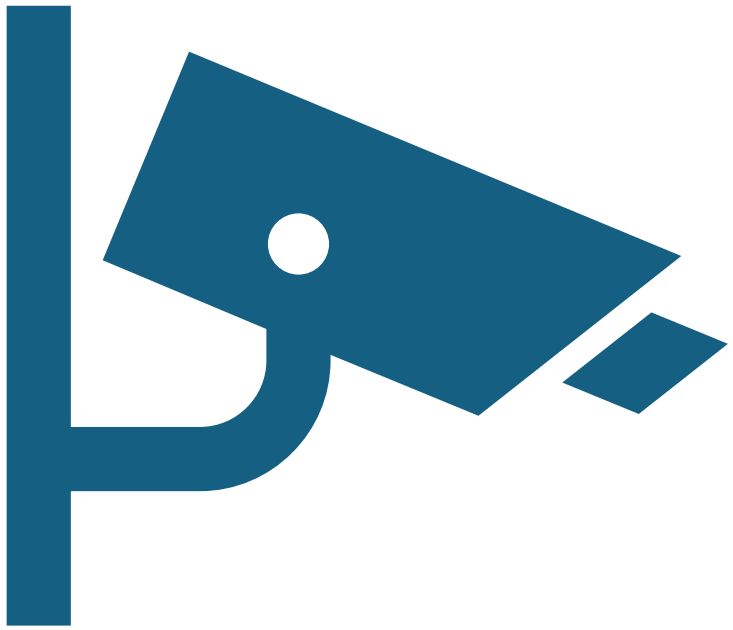
- The right to privacy does not presuppose that one has something shameful to conceal.

Ethical Issues in Privacy vs Security

- Mass surveillance
- Data collection
- Monitoring communications

Balancing Privacy and Security

- Legal
- Necessary
- Proportionate
- Accountable



Surveillance

What is Surveillance?

Surveillance is the monitoring, observation, or collection of data about individuals or groups, typically without their active knowledge.

It is not inherently illegitimate — targeted, judicially authorised surveillance of identified criminal suspects is widely accepted as a legitimate and necessary law enforcement tool.

The ethical and legal debates concern mass surveillance, indiscriminate interception, and the systems built to enable persistent monitoring of entire populations.

Forms of Digital Surveillance

- Targeted Surveillance
- Mass or Bulk Surveillance
- Social Media Monitoring

Lawful Interception

Lawful interception refers to the legally authorised interception of the content of communications by law enforcement or intelligence agencies for investigative or security purposes.

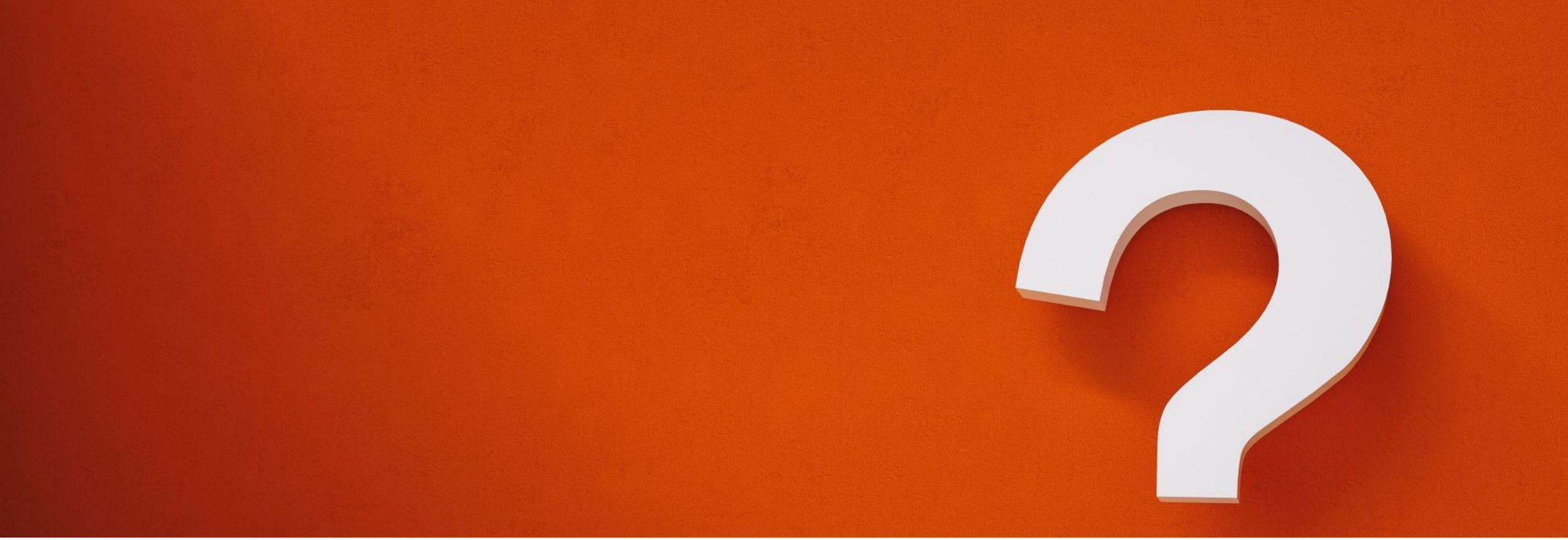
There should be Legal Safeguards

Governments may monitor communications for security and crime prevention.

Cont’d

Risks to Citizen Freedoms

- Reduced privacy
- Self-censorship
- Abuse of power



- Q&A