

209

Data Protection Legislation

The Data Subject

- Most probably you.
- The EU's General Data Protection Regulation (GDPR) defines a 'data subject' as an "identified or identifiable **natural person**" from whom or about whom information is collected.
 - Natural person: a company or organisation cannot be a data subject
- A person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

What should a DPL look like?

▫ Scope

- Individual right to privacy - protect the data subject (the Kenyan citizen)
- The protections offered should be at par with/better than those offered internationally
 - e.g. the obligations of commercial entities when generating/collecting, processing, storing the data.
 - What the state does with your data

What should a DPL look like?

- Specific **limitations** on the rights
 - as per the constitution
- **Clear definition of consent** e.g.:
 - Does silence assume consent?
 - Should I be opted in without my knowledge?

What should a DPL look like?

▫ Data categories

- e.g. how to collect/store/process **sensitive personal data ...**
- i.e. information that can be used to discriminate against you e.g.:
 - information about minors, race, tribe, trade union membership, gender, marital status.

What should a DPL look like?

- Remedies/modes of redress
- A data protection oversight authority and its independence

What should a DPL look like?

- ▣ **Data sovereignty** – data is subject to the laws and governance structures within the nation it is collected.
- ▣ Data sovereignty comes into play when the data is stored outside the country and is subject to that country's laws.

Players

- ▣ **Two entities/persons:**
 - ▣ Data controller
 - ▣ Data processor

Players

- ▣ Data controller
 - ▣ The person or entity that determines
 - the purpose for which personal data is collected and processed
 - the means and method of processing it
- ▣ i.e., dictates how and why data is going to be used by the organisation.

Players

- ▣ **Data processor**
 - ▣ A person/entity that, on behalf of the data controller,
 - ▣ collects personal data
 - ▣ processes this data
 - ▣ Does not own or control the data they process
 - ▣ They can't change the purpose and the means in which the data is used.
 - ▣ They are bound by the instructions given by the data controller.

Players

- ▣ Basically, a **data controller** determines **why and how** personal data should be processed while
- ▣ a data processor carries out these tasks on behalf of the controller.
- ▣ **Example:**
 - ▣ KU may hire a security firm.
 - ▣ The uni determines what information is to be gathered at the gate about the students/staff/other visitors.

Players

- ▣ **Example (cont...):**
 - ▣ The uni is the **data controller** and
 - ▣ The security firm is the **data processor**.
 - ▣ The uni could also **act as both** when collecting other data
 - ▣ e.g. student registration data.
 - ▣ It takes both roles as
 - ▣ it determines the purpose of the data collection and
 - ▣ processes that data itself.

Data Privacy Laws

- Many countries/regions have laws protecting individual's privacy.
- What varies is the comprehensiveness and enforcement of these laws.
- The EU's GDPR is often seen as the gold standard in privacy laws due to its wide scope and stringent enforcement mechanisms.

222

Data Privacy Laws

The EU Context

The EU's GDPR

- The EU has a comprehensive data privacy law known as the General Data Protection Regulation (GDPR).
- A data subject has rights under the GDPR that aim to protect their privacy and right to self-determination.
- The GDPR
 - enhances individuals' control and rights over their personal information
 - simplifies regulations for international business.
 - governs the transfer of personal data outside the EU and the European Economic Area (EEA).

The EU's GDPR - Penalties for Violation

- Severe and designed to be effective, proportionate and dissuasive for each individual case.
- For especially severe violations, listed in Article 83 (5) GDPR, the fine framework can be up to **20 million euros**, or up to **4%** of the organisation's total **global turnover** of the preceding fiscal year, whichever is higher.
- Less severe violations in Article 83 (4) GDPR sets forth fines of up to **10 million euros**, or up to **2%** of the organisation's entire **global turnover** of the preceding fiscal year, whichever is higher.

The EU's GDPR - Penalties for Violation

- **Severe Penalties Examples**
- Facebook's parent company Meta was fined a record-breaking €1.2 billion for transferring data collected from Facebook users in the EU/EEA to the US, violating GDPR international transfer guidelines.
- Amazon was fined €746 million for tracking user data without acquiring appropriate consent from users or providing the means to opt out from this tracking.

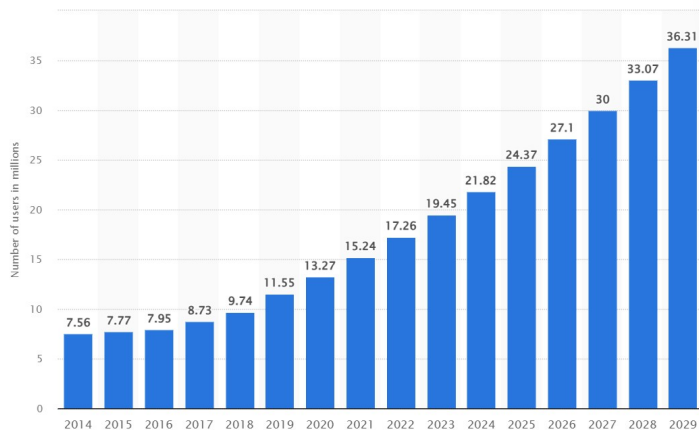
226

Data Privacy

The Kenyan Context

Number of internet users in Kenya from 2014 to 2029
(in millions)

Source: www.statista.com



Web & Mobile Presence Kenya

- Both mobile and internet penetration is very high.
 - According to the Communications Authority (CA, the Kenyan telecommunications industry regulator), in March 2017: 39.1 million mobile subscriptions (86.2% mobile penetration) and 40.59 million internet users (89.4% internet penetration)
 - By December 31, 2022, mobile subscribers were 65.7 million! (we were No 1 in Africa in mobile phone penetration - nearly everyone has more than one device).
 - Millions active on social media daily.
 - Approximately 22.5M Kenyans used the internet in 2023 and by 2028 it will be nearly 39 million (Cowling, 2024).

Data Availability

Technological advances
→
Massive amounts of data
→
Need for data privacy

Kenya's Privacy Laws

- Enshrined in
 - Kenya's constitution and
 - the Data Protection Act
- The constitution protects the right to privacy, including protection against unnecessary revelation of information or infringement of communication
- The Data Protection Act regulates the processing of personal data, provides for the rights of data subjects, and outlines the obligations of data controllers and processors

1. Constitutional Privacy Protections

- The **right to privacy** is enshrined in **Article 31** of the Kenyan constitution:
 - Every person has the right to privacy.
 - This includes the right not to have
 - their person, home or property searched;
 - their possessions seized;
 - information relating to their family or private affairs unnecessarily required or revealed; or
 - the privacy of their communications infringed.

(Kenyan Constitution: Chapter Four, Part 2, Article 31)

Further...

- **Article 2:** should Kenya sign/ratify international treaties/ conventions they become part of the Kenyan domestic law.
- Kenya is a signatory to
 - the Universal Declaration of Human Rights (UDHR)
- and has ratified
 - the International Covenant on Civil and Political Rights (ICCPR)
- They include privacy rights.

Limitations to Privacy Rights (Kenya)

- **Article 24 (3)** requires anyone wishing to limit any fundamental right to justify themselves.
- They must identify the need...

Limitations to Privacy Rights (Kenya)

- E.g. don't just say you are fighting terrorism
 - Terrorism should be no excuse for poor governance
- Provide a specific reason for the data collection:
 - Avoid data collection for the sake of data collection
 - E.g. only take my DNA information only after I commit a crime
- Reason usually given is "to provide government services"
 - To business entities?

Limitations to Privacy Rights (Kenya)

- Remember:
- A Kenyan's right to privacy includes the right NOT to have "information relating to their family or private affairs **unnecessarily required or revealed**; ..."

Limitations to Privacy Rights (Kenya)

- Our personal information may be collected/processed/shared etc ...
- **...only if article 24 of the Constitution is adhered to.**
 - Justify/id the need.
- Our rights and fundamental freedoms may be limited **"for the purposes, in the manner and to the extent"** set out in Article 24 of the Constitution...

Limitations to Privacy Rights (Kenya)

- **Limited for the purposes...**
 - E.g. such restrictions may only be imposed for purposes of respecting others' rights/reputations, or national security, public order, public health or morals.
- **...in the manner...**
 - Restrictions/limitations to our right to privacy must be legal and follow due process
 - e.g. acquisition of warrants.
- **...to the extent...**
 - such restrictions must not only be necessary but also proportionate.
 - NOT some people shot up a mall, let's gather ALL information about ALL people

Data Privacy Laws

- A **data protection law** serves to act as a framework that provides guidelines on personal data:
 - Who the **data controller** is
 - Who **processes** the data.
 - How/why/where the data is processed.

Data Privacy Laws

- Data is a right; a human right ...
- i.e. it is a right attached to a human;
- not property/a business asset
 - You are a person, you are not your data.
 - Sure, I can extract patterns from your data and make decisions based on them but you're human, not a game of chess.
 - Decisions should not be automatically made based on your data.

2. The Kenya Data Protection Act, 2019

- Governs how personal data is collected, processed, and transferred, both within Kenya and internationally.
- Expedited following concerns raised over the Huduma Namba registration exercise.
 - the safety of citizens' personal data collected by the Government.

2.1 Purpose of the Act

- gives effect to Article 31(c) and (d) of the Constitution
 - (the right every person has not to have (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed.)
- establishes the Office of the Data Commissioner
- regulates the processing of personal data

2.1 Purpose of the Act

- provides for the
 - rights of **data subjects** (individuals whose data is being processed)
 - obligations of **data controllers** (those who determine the purpose and means of processing of personal data) and
 - the obligations of **data processors** (those that process personal data on behalf of the data controller)

2.2 Data Protection Principles

- Data Controllers and Processors must:
 - process data lawfully;
 - minimise collection of data;
 - restrict further processing of data;
 - ensure data quality;
 - establish and maintain security safeguards to protect personal data.

The Data Protection Act of 2019

- Law to safeguard citizens' personal data.
 - Sets out comprehensive provisions for the collection, use, storage, and handling of personal data.
 - seeks to promote and protect the privacy of personal data and ensure that data controllers, data processors, and data subjects adhere to the highest standards of data protection.
 - sets out stringent requirements for data controllers on what to do with the personal data they collect...

The Data Protection Act of 2019

- They must provide data subjects with a notice explaining how their data will be collected, processed, and stored.
- They must include details on the purpose of the data processing, the legal basis for the data processing, and the party to whom the data will be disclosed.
- Data controllers must also obtain explicit consent from data subjects before they can process their personal data.
- They must ensure that they only collect and process data that is necessary for the purpose they seek to achieve.

The Data Protection Act of 2019

- The Data Protection Act also gives data subjects the right to access their personal data held by data controllers.
- Data subjects can request data controllers to provide them with a copy of their personal data, and data controllers must respond to these requests **within thirty days**.
- Data subjects can also request data controllers to rectify, delete, or restrict the processing of their personal data.
- Data controllers must comply with these requests, except under specific circumstances set out in the Act.

The Data Protection Act of 2019

- The Act also provides for the protection of data subjects' rights against unauthorised processing, loss of data, or destruction of data.
- Data controllers must take appropriate measures to safeguard personal data, including measures to prevent unauthorised access, modification, disclosure, or destruction of personal data.
- Data controllers must also put in place adequate technical and organisational measures to ensure the security of personal data.

The Data Protection Act of 2019

- The act establishes the office of the **Data Protection Commissioner**, who is responsible for overseeing and enforcing data protection regulations in Kenya.
- The Commissioner has the power to investigate data controllers and processors suspected of violating data protection laws and to impose sanctions on violators of the law.

The Data Protection Act of 2019

- Regulates the processing of personal data and information.
- GDPR principles informed the bill on the governance of this information
 - How it is handled, stored and shared.
- Illegal processing of personal data is punishable by law.
 - Upto 3,000,000/= fine or a maximum of 2 years in jail.

The Data Protection Act of 2019

- You have the right to know how your information is handled.
- You have the right to request your personal data be deleted/edited if it is inaccurate.
- The right to data portability is enforced.
 - A data subjects can obtain data that a data controller holds on them and reuse it for their own purposes.
 - You now have the right to refuse an organisation to transfer your personal data to another organisation.
 - Should be a relief to cellphone users.

The Data Protection Act of 2019

- To paraphrase an ICT CS:
- KQ, tourist hotels etc must comply when handling personal data from clients.
- Also phone-based lenders such as Safaricom, who gather tons of personal data through services offered jointly with local banks.

2.3 Registration of Data Controllers and Processors

- All data controllers and data processors must be registered with the Data Commissioner.
- They must register themselves and renew their registration every 3 years.

2.4 Transfer of Personal Data Outside Kenya

- All data controllers/data processors must ensure at least one copy of personal data to which the Act applies is stored on a server or data centre located in Kenya
- Cross-border processing of sensitive personal data is prohibited
 - the transfer of personal data to foreign countries or international organisations is only allowed when certain conditions are met or under certain circumstances specified in the Act...

2.4 Transfer of Personal Data Outside Kenya

- The following conditions ensure that cross-border data processing is carried out with proper safeguards and consideration for data subjects' rights and privacy.
 1. Adequate Protection
 2. Consent
 3. Legal Obligations
 4. Vital Interests
 5. Public Interest
 6. Legal Claims

2.4 Transfer of Personal Data Outside Kenya

- **Adequate Protection:** if the foreign country or organisation ensures an adequate level of protection for the data.
 - the receiving entity must have data protection laws or mechanisms in place that are equivalent or similar to those in Kenya.

2.4 Transfer of Personal Data Outside Kenya

- **Consent:** if the data subjects have provided explicit and informed consent for their data to be transferred abroad.
 - This consent must be obtained before the data transfer takes place.

2.4 Transfer of Personal Data Outside Kenya

- **Legal Obligations:** if such transfers are necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken at the data subject's request ...

2.4 Transfer of Personal Data Outside Kenya

- **Example:**
 - A cloud service provider, hosting sensitive data for various clients, is **legally obligated** to implement strict security measures to protect the confidentiality and integrity of the data.
 - To comply with these legal obligations, the provider regularly conducts security audits, encryption of stored data, and access control measures.
 - They must also report any data breaches promptly to both their clients and relevant authorities, as required by data protection regulations.
 - These legal obligations ensure the safety and privacy of client data stored on their servers.

2.4 Transfer of Personal Data Outside Kenya

- **Vital Interests:** if the data transfers are necessary to protect the vital interests of the data subject, particularly in life-threatening situations.
- The processing of personal data may be necessary to protect the person's life or physical health in e.g.
 - medical emergencies,
 - natural disasters, or
 - situations where an individual's life is in immediate danger.

2.4 Transfer of Personal Data Outside Kenya

- **Vital Interests Example:**
 - If you are unconscious and admitted to a hospital, medical professionals may process your personal data without consent if it is necessary to provide life-saving treatment.

2.4 Transfer of Personal Data Outside Kenya

- **Public Interest:** if the data transfers are necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
 - e.g., to conduct a public health survey during a disease outbreak.
 - This is done in the public interest to protect the health of the population.

2.4 Transfer of Personal Data Outside Kenya

- **Legal Claims:** Transfers of data may be allowed if they are necessary for the establishment, exercise, or defense of legal claims.
 - E.g. a law firm processes personal data without consent to pursue a legal claim on behalf of a client in a court case.
 - This processing is necessary for the establishment, exercise, or defense of legal claims ...

2.4 Transfer of Personal Data Outside Kenya

- ❑ **Legal Claims Example:**
- ❑ A software company is facing a legal dispute with a former employee who claims they were wrongfully terminated.
- ❑ To defend themselves, the company needs to gather evidence related to the employee's performance, attendance records, and communication logs during their employment.
- ❑ This involves **collecting personal data**, such as the employee's work-related emails, attendance records, and performance evaluations.
- ❑ The company processes this personal data without the explicit consent of the former employee, as it's necessary for the defense of their legal claim against the wrongful termination allegation.

2.5 Exemptions

- ❑ The processing of personal data is exempt from the provisions of the Data Protection Act;
- ❑ for national security or public order reasons;
- ❑ when disclosure is required by or under any written law or by an order of the court.

How DPL Is Enforced in Kenya

- ❑ Through the Data Protection Act and various regulations that operationalise the provisions of the Act.
- ❑ **The Data Protection (Compliance and Enforcement) Regulations, 2021** outline the compliance and enforcement provisions for the
 - ❑ Data Commissioner,
 - ❑ Data Controllers, and
 - ❑ Data Processors.

How DPL Is Enforced in Kenya

- ❑ **A Data Protection Commissioner** serves as the Data Protection Authority that:
 - ❑ registers organisations / businesses that own, manage, or control data.
 - ❑ investigates data infringements

The Kenyan Data Commissioner's Roles

When walking through a college campus, it is hard to spot someone without a phone in their hand. Whether it's a group of sorority sisters taking a group selfie, a grad student walking to class listening to music or a freshman scrolling through Instagram, smartphones have become an unavoidable staple in the lives of college students.

❑ (Kuzel, 2020).

The Kenyan Data Commissioner's Roles

- The ODPC (Office of the Data Protection Commissioner) ensures that personal data is handled responsibly and that individuals' privacy rights are upheld.
- They do this via the following 11 roles ...

The Kenyan Data Commissioner's Roles

1. Oversee the **implementation** of and be responsible for the **enforcement** of the Data Protection Act.
2. Establish and maintain a **register** of data controllers and data processors.

The Kenyan Data Commissioner's Roles

3. Exercise **oversight** on data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with the Act.
4. Promote **self-regulation** among data controllers and data processors.

Homework: Privacy by Design

- Privacy by Design is a framework emphasising the integration of privacy and data protection into the design and operation of systems, technologies, and business practices from the outset, rather than as an afterthought.
- As a systems developer you should consider and incorporate privacy into your development process in a proactive manner, ensuring that personal information is protected at every stage of the lifecycle of data.
- Your task is to get really familiar with the Privacy by Design principles, which align with the concept of self-regulation in data protection.

The Kenyan Data Commissioner's Roles

5. Conduct an **assessment**, on its own initiative or at the request of a private or public body, for the purpose of ascertaining whether information is processed according to the provisions of this Act or any other relevant law.
6. Receive and **investigate any complaint** by any person on infringements of the rights under this Act.

The Kenyan Data Commissioner's Roles

7. Take such measures as may be necessary to bring the provisions of this Act to the **knowledge of the general public**.
8. Carry out **inspections** of public and private entities with a view to evaluating the processing of personal data.

The Kenyan Data Commissioner's Roles

9. Promote **international cooperation** in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements.
10. Undertake **research** on developments in data processing of personal data and ensure that there is **no significant risk or adverse effect** of any developments on the privacy of individuals.

The Kenyan Data Commissioner's Roles

11. Perform such **other** functions as may be prescribed by any other law or as necessary for the promotion of the object of this Act.

How DPL Is Enforced in Kenya... (cont)

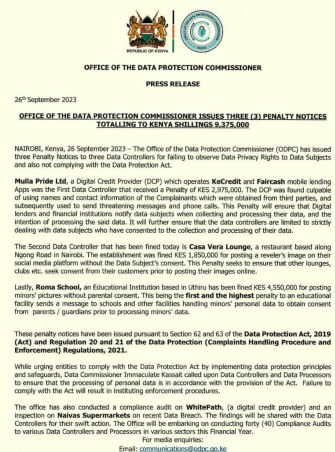
- The Act requires that any person who acts as a **data controller or data processor** must be registered with the Data Commissioner.
 - ... and renew their registration every 3 years.
- Every data controller or data processor is required to ensure the storage, on a server or data centre located in Kenya, of at least one serving copy of personal data to which the Act applies.

How DPL Is Enforced in Kenya

- Cross-border processing of sensitive personal data is prohibited and only allowed when certain conditions are met or under certain circumstances specified in the Act.
- In case of non-compliance with these regulations, penalties may be imposed.

Case Studies

Data Protection Enforcement Actions in Kenya - September 2023



Introduction

- In September 2023, Kenya witnessed a series of significant data protection enforcement actions aimed at upholding the Kenya Data Protection Act, 2019 (KDPA) and its associated regulations.
- These actions serve as a clear message to data controllers and processors regarding the importance of safeguarding personal data and adhering to privacy regulations.
- Let's delve into the notable cases and the regulatory provisions involved.

Case 1: Digital Credit Provider's Penalty

- **Background**
- A Digital Credit Provider (DCP) operating two mobile lending apps faced unprecedented consequences for its handling of personal data.
- They gained the dubious distinction of being the first Data Controller to incur a substantial penalty, totaling almost 3 million Kenyan shillings.

Case 1: Digital Credit Provider's Penalty

- **Violation**
- The DCP was penalised for acquiring the names and contact information of complainants through third parties, and subsequently utilising this data to send threatening messages and make intimidating phone calls.
- This action directly contravened the provisions of the **Kenya Data Protection Act (KDPA), 2019**, specifically **Sections 62 and 63**.

Case 1: Digital Credit Provider's Penalty

- **Enforcement Measures**
- To ensure compliance with the **KDPA and the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021** (regulations 20 and 21), the following measures were enforced ...

Case 1: Digital Credit Provider's Penalty

- **Data Subject Notification:**
 - Digital lenders and financial institutions must notify data subjects when collecting and processing their data.
 - Transparency in data handling is essential for protecting individuals' privacy.
- **Consent Requirement:**
 - Data controllers are obligated to process personal data only after obtaining **explicit consent** from data subjects.
 - This consent-based approach enhances data protection and ensures individuals' rights are respected.

Case 2: Restaurant's Privacy Infringement

- **Background**
- A Nairobi-based restaurant found itself in legal trouble, facing a fine of nearly 2 million Kenyan shillings.
- The restaurant had posted a customer's image on its social media platform without obtaining the necessary consent.

Case 2: Restaurant's Privacy Infringement

❑ Violation

- ❑ The restaurant's actions constituted a breach of the data subject's privacy rights.
- ❑ Posting personal images without consent contradicts the principles of data protection outlined in the KDPA.

Case 2: Restaurant's Privacy Infringement

❑ Enforcement Measures

- ❑ The penalty imposed on the restaurant highlights the importance of respecting data subjects' privacy rights.
- ❑ It is hoped that going forward, such establishments (restaurants, lounges, clubs, etc) will strive to seek consent from customers before posting their images online.

1. Signature of Applicant:

 (My signature also gives/does not give permission for any photo of myself to be used for any promotion or media coverage relating to _____ Conference and for my name TO BE USED/NOT TO BE USED.

Case 3: School's Data Protection Violation

❑ Background

- ❑ A school faced severe consequences when it was fined over 4.5 million Kenyan shillings for posting pictures of minors without their parents' consent.
- ❑ This case underscored the significance of protecting minors' personal data.

Case 3: School's Data Protection Violation

❑ Violation

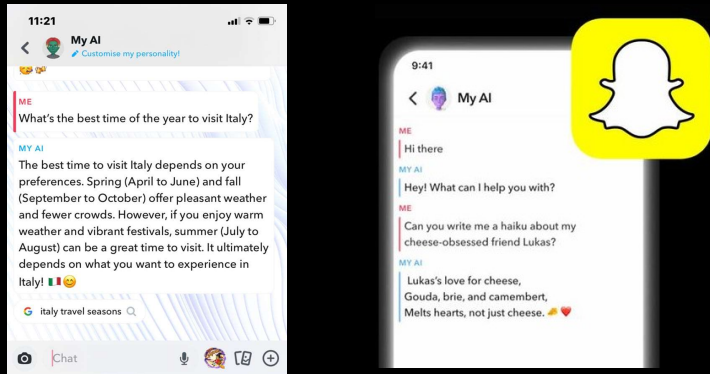
- ❑ The school's actions violated the privacy of minors.
- ❑ Before processing personal data related to minors, schools and similar institutions handling such data must obtain explicit consent from parents or legal guardians.

3. Signature of Parent/Guardian: (for applicants under 18 years of age as at 27th

I _____, Parent/Guardian of _____
 _____ give my permission
 for _____ to attend the _____
 _____ Conference in _____ and nominate _____
 _____ as the adult responsible for the care of my child
 during this event and GIVE/DO NOT GIVE PERMISSION for a photo of my child to be
 used and named for any promotion or media coverage relating to _____

 SIGNATURE OF PARENT/GUARDIAN: _____ DATE: _____

On A Separate But Related Note:



On A Separate But Related Note: Snapchat's AI Chatbot Feature: "My AI"

- ❑ Powered by OpenAI's ChatGPT technology.
- ❑ The UK's data protection regulator, the Information Commissioner's Office (ICO) raised concerns about the privacy risks *My AI* poses to children.
- ❑ Investigating how *My AI* processes the personal data of Snapchat's 21 million UK users, including children aged 13-17.

On A Separate But Related Note

- ❑ Findings suggest a potential failure by Snapchat to properly identify and evaluate privacy risks to children before releasing *My AI* in April, 2023.
- ❑ These findings do not necessarily mean that Snapchat has violated British data protection laws.
- ❑ The ICO is considering the company's response before making any final enforcement decision ...

On A Separate But Related Note

- ❑ Snapchat's response:
 - ❑ *My AI* went through robust legal and privacy reviews before launch
 - ❑ it is reviewing the ICO's notice
 - ❑ it is committed to user privacy
 - it is committed to working with the ICO to ensure that their risk assessment procedures align with privacy standards.
- ❑ If Snapchat does not adequately address its concerns, *My AI* could be banned in the UK.

On A Separate But Related Note

- ❑ The investigation highlights growing regulatory scrutiny over the use of AI (e.g. chatbots) and privacy risks, especially for children's data.
- ❑ It also emphasises the role of regulatory bodies like the ICO (and our very own ODPC) in assessing and addressing potential privacy risks associated with new technologies.

Back to our case study ...

Data Protection Enforcement Actions in Kenya - September 2023

Data Commissioner's Office Initiatives

- In addition to the enforcement actions, the Data Commissioner's office revealed several ongoing initiatives aimed at ensuring data protection compliance ...

Data Commissioner's Office Initiatives

- **Compliance Audits:**
 - The Data Commissioner's office was conducting a compliance audit on a second Digital Credit Provider (DCP).
 - This emphasises the importance of adhering to data protection regulations within the financial sector.

Data Commissioner's Office Initiatives


- **Inspection on a Supermarket**
 - The office was also conducting an inspection on a popular supermarket regarding recent data breaches.
 - The findings would be shared with the Data Controllers for prompt corrective action.

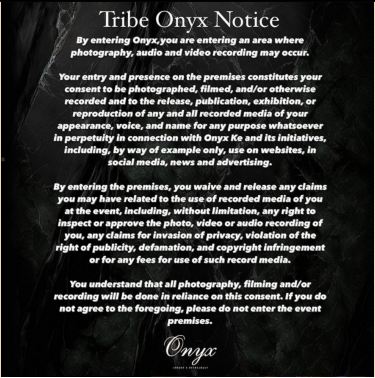
Data Commissioner's Office Initiatives

- **Upcoming Compliance Audits:**
 - The ODPC plans to conduct 40 compliance audits across various sectors during the current financial year.
 - This proactive approach underscores a commitment to enforcing data protection regulations in Kenya.

Lessons That Ought to Be Obvious

- The Kenya Data Protection Act, 2019 is not a joke.
- These cases highlight the consequences of non-compliance with the KDPA and its associated regulations.
- Organisations and institutions that handle personal data **MUST** prioritise transparency, consent, and compliance with data protection laws to protect the privacy of data subjects effectively.

	<p style="text-align: center;">NOTICE</p> <p style="text-align: center;"><small>YOU ARE ENTERING AN AREA WHERE PHOTOGRAPHY, AUDIO AND VIDEO RECORDING MAY OCCUR. PLEASE BE AWARE THAT BY ENTERING THE EVENT PREMISES YOU CONSENT TO BE PHOTOGRAPHED, FILMED, AND/OR OTHERWISE RECORDED WITHOUT COMPENSATION AND WAIVE AND RELEASE ANY CLAIMS YOU MAY HAVE RELATED TO THE USE OF RECORDED MEDIA OF YOU AT THE EVENT FOR ANY PURPOSE WHATSOEVER IN PERPETUITY IN CONNECTION WITH QUIVER LOUNGE & GRILL, BY WAY OF EXAMPLE, USE ON WEBSITE, IN SOCIAL MEDIA, NEWS AND ADVERTISING OR FOR ANY PAYMENT FOR USE OF SUCH RECORDED MEDIA</small></p> <p style="text-align: center;"><small>DO NOT ENTER THIS AREA IF YOU DO NOT AGREE TO THE FOREGOING</small></p> <hr/> <p style="text-align: center;"><small>TUNAOMBA MUELEWA KWAMBA KWA KUINGIA ENED HILI, UNAKUBALI KUPIGWA PICHA, BILA KULIPWA, NA UNATOA RUHUSA KWA PICHA YAKO KUTUMIKA KATIKA FILAMU, MATANGAZO, KANDA NA KUTUMIKA KATIKA VYOMBO VYA HABARI. WENYE ENED HILI NA WADHAMINI WA SHIGHILI HII HAWATOWAJIBIKA NA JAMBO LA AINA YOVOTE AMBALO LITATOKEA</small></p> <p style="text-align: center;"><small>TAFADHALI USINGIE ENED HILI KAMA HUKUBALIANI NA YALE YATAKADENDELEA HAPA</small></p> <p style="text-align: center;"></p>
	<p>Turns Out “Obvious” Is Relative</p>
	<p>Data controllers almost immediately struck back with warnings of implied consent to revellers entering their premises.</p>



Copycat behaviour sprouted all over the place.

Tribe Onyx Club, Texas Barbeque ...

Can Data Controllers Do This?

- ❑ We appreciate this company's "proactive" approach to addressing data protection and privacy concerns.
- ❑ However.
- ❑ We can also provide some insights based on the KDPA, 2019, and the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 ...

Can Data Controllers Do This?

- ❑ It's nice of them to inform individuals about the possibility of being photographed, filmed, or recorded.
- ❑ Such notices MUST however align with the KDPA to protect individuals' rights effectively.
- ❑ We can suggest a few considerations to enhance the notice's compliance with data protection regulations ...

Relevant Data Protection Regulations: Explicit Consent

- ❑ The notice mentions that individuals entering the event premises "consent" to be photographed, filmed, and recorded.
- ❑ Under KDPA, **explicit consent** should be obtained
 - ❑ individuals must provide a **clear and unambiguous agreement**.
- ❑ It's advisable to rephrase the notice to explicitly state that individuals entering the premises **have the option to provide or withhold consent**.

Relevant Data Protection Regulations: Purpose Limitation

- ❑ The notice mentions the use of recorded media for "any purpose whatsoever."
- ❑ KDPA requires that personal data be collected for specific, legitimate purposes and not used in a manner incompatible with those purposes.
- ❑ The company should specify the intended purposes for which the recorded media will be used, such as promoting its events.

Relevant Data Protection Regulations: Duration of Consent

- ❑ The notice states that individuals waive and release any claims "in perpetuity."
- ❑ KDPA requires that the duration of consent be limited to what is necessary for the specified purposes.
- ❑ They should consider specifying a reasonable timeframe for which consent is valid to align with data protection principles.

Relevant Data Protection Regulations: Opt-Out Option

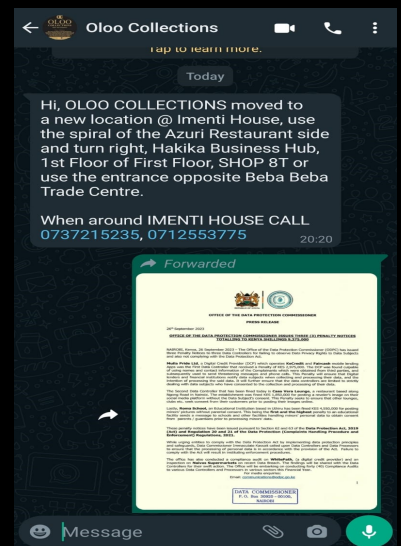
- ❑ The notice mentions that individuals should not enter the area if they do not agree to the terms.
- ❑ While this is a valid approach, it's also advisable to provide an opt-out mechanism for individuals who initially consented but later wish to withdraw their consent.

Relevant Data Protection Regulations

- ❑ Data protection compliance is essential in today's digital age
- ❑ The company should review and refine this notice to ensure that:
 - ❑ it complies with data protection regulations
 - ❑ while still serving the intended purpose of informing individuals about potential recording activities.
- ❑ This approach will help create a more transparent and privacy-conscious environment for event attendees.

- ❑ For more examples and analyses, cf Document titled:
 - ❑ *Data Protection Guidelines on Event Photography - Regulatory Alert*

Kenyans On Social Media also responded to the ODPC's press release.



Kenyans On Social Media also responded to the ODPC's press release.

Sidenote: Points To Consider

- ❑ You can play your part in spreading the gospel of data privacy (esp on social media) without being boring about it.
- ❑ Humour can be a powerful way to address complex issues.
- ❑ Let's consider the underlying message and implications of *akina* the Emojis ...

Points To Consider

- ▣ **Privacy Awareness**
- ▣ Conceal individuals' faces with emojis suggests an increased awareness of privacy concerns.
- ▣ We are acknowledging that individuals may not want their images to be shared publicly without their consent.

Points To Consider

- ▣ **Social Commentary**
- ▣ On the fines and penalties imposed on businesses for privacy violations.
- ▣ Highlights the importance of respecting individuals' privacy rights, even in casual settings.

Points To Consider

- ▣ **Encouraging Consent**
- ▣ The act of covering faces with emojis indirectly emphasises the importance of obtaining consent before capturing and sharing images of individuals.
- ▣ It serves as a reminder that consent should be sought in various social and business contexts.

Points To Consider

- ▣ **Engagement and Discussion**
- ▣ Such a pic can spark discussions about privacy and data protection.
- ▣ It encourages people to think about their rights and the responsibilities of data controllers.

Points To Consider

- ▣ **Balancing Privacy and Expression**
- ▣ While humor can be a useful tool, it's essential to strike a balance between privacy protection and freedom of expression.
- ▣ While individuals have the right to privacy, they also have the right to express themselves and share experiences.

DPL Comparisons

Enforcement of DPL: Kenya vs EU

- The Data Commissioner in Kenya plays a crucial role in enforcing data protection laws.
- In comparison, EU's GDPR is enforced by each member state's *national data protection authority* ...

Enforcement of DPL: Kenya vs EU

- These authorities are independent public authorities that *supervise*, through investigative and corrective powers, the *application* of the data protection law.
- They provide expert *advice* on data protection issues and *handle complaints* lodged against violations of the GDPR and the relevant national laws.
- There is one such authority in each EU Member State.

Enforcement of DPL: Kenya vs EU

- Like Kenya's Data Commissioner, these authorities have powers to
 - carry out *investigations* in the form of data audits,
 - issue *warnings* for non-compliance,
 - issue *corrective measures* such as bans on processing and fines.

Enforcement of DPL: Kenya vs EU

- Unlike Kenya where there is a single Data Commissioner, GDPR enforcement can vary by member state as each state has its own national data protection authority.

327

Data Privacy

The American Context

The United States

- No comprehensive data privacy law (unlike us and the EU).
- Instead, various federal and state laws that cover different aspects of data privacy, like health data, financial information, or data collected from children.
 - Federal laws include: ECPA, FERPA, GLBA, FCRA, HIPAA, COPPA, and VPPA ...

The United States

- **ECPA (Electronic Communications Privacy Act)**
- Governs the privacy of electronic communications, including email, telephone conversations, and data stored electronically.
- **FERPA (Family Educational Rights and Privacy Act)**
- Protects the privacy of student education records. It gives parents and eligible students certain rights regarding the release of student records.

The United States

- **GLBA** - Gramm-Leach-Bliley Act: requires financial institutions to explain their information-sharing practices to customers and safeguard sensitive financial information.
- **FCRA** - Fair Credit Reporting Act: regulates the collection, dissemination, and use of consumer credit information, including credit reports and credit scores.

The United States

- **HIPAA** (Health Insurance Portability and Accountability Act)
- Establishes standards for the privacy and security of protected health information (PHI) to protect patients' medical records and other health-related data.
- **COPPA** (Children's Online Privacy Protection Act)
- Imposes requirements on websites and online services that collect personal information from children under the age of 13.

The United States

- **VPPA** (Video Privacy Protection Act)
- Restricts the disclosure of an individual's video rental or sales records without their consent.
- May have been established in 1988 when video stores were a thing but still very relevant and effective today in the age of video streaming.
- Protects Americans' video consumption data.

The United States

- Thus the U.S. lacks a comprehensive federal privacy regulation.
- States like California have started implementing their own privacy laws, creating a patchwork of regulations.
 - Complying with multiple state privacy laws and evolving regulations is complex.
 - E.g., organisations must adapt to frequent changes in breach notice laws
 - aka data breach notification law that require organisations to notify individuals and relevant authorities when a data breach occurs.
 - typically specify the timeframe, content, and method of notification.

334

Data Privacy

The Chinese Context

China

- Personal Information Protection Law (PIPL) and the Data Security Law.
- The PIPL
 - China's first comprehensive law designed to regulate online data and protect personal information.
 - Draws from the EU's GDPR
 - Heavy penalties if broken.

Challenging Data Privacy Issues

Challenging Data Privacy Issues

- Embedding Data Privacy: It must be integrated into the core of an organisation's data strategy.
 - E.g. failure to prioritise data privacy led to the Facebook-Cambridge Analytica scandal.
- Device Proliferation: The rise of IoT devices and BYOD policies complicates data management and may pose security risks.
 - E.g. employees bringing personal IoT devices (Fitbits, Alexa etc)to work may inadvertently expose sensitive data.
 - Unauthorised IoT devices may collect and share sensitive workplace data.

Challenging Data Privacy Issues

- Increasing Maintenance Costs: Securing systems is expensive, but data breaches are costlier.
 - E.g. investing in automation reduces the cost of managing data privacy.
- Access Control Challenges: Poor access management often leads to data breaches.
 - E.g. inadequate user access control can result in unauthorised data access.

Challenging Data Privacy Issues

- Data Visibility: Organisations must know where sensitive data is located.
 - E.g. data classification tools help identify and protect sensitive information.
- Building a Good Data Culture: Prioritising data value over data volume reduces security risks.
 - E.g. companies with excessive data storage may face higher security risks.

Challenging Data Privacy Issues

- Managing the Scale of Data: As data volume grows, organisations need scalable solutions.
 - E.g. cloud storage solutions are scalable and can handle vast amounts of data.
- Regulatory Complexity: Compliance with various privacy laws requires efficient processes.
 - E.g. GDPR introduced new challenges for organisations, including the need for data protection officers.
 - Finding qualified individuals who possess legal, technical, and organisational skills for the role is a challenge.

Challenging Data Privacy Issues

- ❑ Third Parties: Many organisations use third-party vendors, increasing data security risks.
 - ❑ Data breaches often occur due to third-party vulnerabilities.
- ❑ Untested Security Plans: Organisations must regularly test security and incident response plans.
 - ❑ Failing to test incident response plans can lead to chaos during a security breach.

Challenging Data Privacy Issues

- ❑ Component Manufacturers: The origin of components used in devices raises national security concerns.
 - ❑ It's essential to know the source and security of components used in critical systems.
- ❑ Ever-Changing Risks: The dynamic nature of hacking threats necessitates continuous learning.
 - ❑ Security professionals must stay updated to counter evolving cybersecurity threats.

Challenging Data Privacy Issues

- ❑ Unclear or Impractical Policies: Policies must be both clear and feasible for effective implementation.
 - ❑ Policies written in technical jargon may lead to misunderstandings.
- ❑ E.g.:

"Unauthorised individuals attempting to access the system will be met with robust countermeasures, including but not limited to rigorous intrusion detection protocols, real-time threat analysis, and immediate implementation of stringent security measures."

Challenging Data Privacy Issues

- ❑ Technically accurate policy.
- ❑ However, it has complex jargon and vague terms ("robust countermeasures", "stringent security measures").
- ❑ This may lead to misunderstandings among non-technical staff.
- ❑ **Quick Exercise:**
- ❑ Make this particular policy clearer and more accessible
 - ❑ specify the exact security measures and procedures to be followed in plain language ...

Challenging Data Privacy Issues

"Unauthorised individuals attempting to access the system will be met with robust countermeasures, including but not limited to rigorous intrusion detection protocols, real-time threat analysis, and immediate implementation of stringent security measures."

"Anyone who tries to access the system without permission will face strong security measures. These include things like our system checking for unauthorised access, constantly monitoring for threats, and taking quick action to make sure our security stays tight."

Best Practices in Privacy and Security:

- ❑ Education: Promote a culture of security within organisations.
 - ❑ E.g. teach employees to validate emails, perform backups, and use two-factor authentication.
- ❑ Continuous Learning: Security professionals should stay updated through associations, podcasts, and webinars.
 - ❑ E.g. membership in organisations like the Information Systems Audit and Control Association (ISACA) or the Information Systems Security Association (ISSA) provides valuable resources.

Best Practices in Privacy and Security:

- ❑ Basic Cybersecurity: Prioritise fundamental cybersecurity measures.
 - ❑ E.g., effective password management and network security are basic but critical.
- ❑ Third-Party Oversight: Establish strong oversight of third-party vendors.
 - ❑ Due diligence as 3rd party vulnerabilities can lead to data breaches

Best Practices in Privacy and Security:

- ❑ Holistic Security: Embrace a comprehensive security mindset.
 - ❑ E.g. acknowledge that complete security is unattainable but aim for resilience:
 - ❑ e.g., regular data backups/recovery, well defined incident response plans in case of security breaches, advanced security monitoring tools and systems, staff training etc
- ❑ Physical Security: Include physical security measures in information security strategies.
 - ❑ E.g. privacy filters on screens and awareness of conversations in public places.

Outro

- ❑ No one wants to live in places of uncontrolled terror and/or violence.
- ❑ However...
- ❑ No one wants to live in a world of uncontrolled surveillance

Outro

- ❑ Privacy is a **fundamental right** that encompasses various aspects of our lives.
- ❑ It is a multifaceted issue with legal, ethical, and social dimensions.
- ❑ It's protected by
 - ❑ laws and
 - ❑ ethical principles
- ❑ However, technological advancements and evolving privacy challenges require ongoing attention and debate.

Outro

- ❑ Balancing technological advancements, legal obligations, and societal concerns is an ongoing challenge.
 - ❑ Balancing the need for privacy with other societal interests, such as security and public safety, is an ongoing challenge.
- ❑ Organisations must prioritise privacy, adopt best practices, and adapt to the evolving landscape of data privacy and security.

Outro

- ❑ Laws and ethical guidelines **evolve** to address these issues.
- ❑ However, the rapid pace of technological change often **outpaces** regulatory responses.
- ❑ This makes privacy a continually evolving topic of discussion and debate.

Task

353

- **Privacy? I've nothing to hide!**
- Glenn Greenwald is a journalist who reported on the Edward Snowden files.
- These exposed the US government's massive surveillance of private citizens.
- Watch his TED Talks video: **Why privacy matters**
- <https://www.youtube.com/watch?v=pcSlowAhvUk>

References

- Burgess, M. (2019, February 14). What is GDPR? The summary guide to GDPR compliance in the UK. Retrieved from <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>
- Kiprono, D.: Right to privacy must be protected. (2018, April 28). Retrieved from <https://www.nation.co.ke/oped/opinion/Why-right-to-privacy-must-be-protected-in-digital-age/440808-4535004-cd3jnw/>
- Lex - 31995L0046 - EN. (1995). Retrieved from <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>
- M a s o n , R . O https://www.researchgate.net/publication/242705009_Four_Ethical_Issues_of_the_Information_Age
- Privacy International. (2019, January). State of Privacy Kenya. Retrieved April 29, 2019, from <https://privacyinternational.org/state-privacy/1005/state-privacy-kenya>
- Venezuela: Guaidó calls on people to take to the streets [Audio blog post]. (2019, April 30). Retrieved April 30, 2019, from <https://www.bbc.co.uk/programmes/p077x4xr>

PROFESSIONAL ETHICS IN COMPUTING

Case Study 1

Case Study 1

- Oti works as a data scientist at SocialSpace, a social media company.
- He has access to a large amount of confidential user data that includes personal information like names, locations, ages, interests, and browsing history.
- One day, Oti's BFF Kevo, who works for an advertising agency, asks him to share some user data with him so he (Kevo) can improve his ad targeting algorithms.
- Kevo promises he won't misuse the data.
- Oti is tempted because he wants to help his friend.

The Ethical Dilemma

- This scenario poses an ethical dilemma for Oti.
- Sharing user data without permission
 - violates the users' privacy and
 - the confidentiality agreement Oti has with SocialSpace.
- However, he feels **loyalty** to his friend and thinks the data could remain anonymous.

The Ethically Correct Decision

- Whichever school of thought you subscribe to in terms of moral philosophies/ethical theories ...
 - ...Oti should not share the confidential data.
- Protecting user privacy should take **priority** over helping a friend ...

The Ethically Correct Decision

- SocialSpace trusts him with the data, and he has a **duty** to honour that trust.
- While the **benefits** to his friend or the ad agency may seem worthwhile, the **risks** of harming users and violating ethics codes outweigh them.
- Even if Oti anonymises the data, sharing it for unauthorised purposes goes against his **professional principles**.

The Ethically Correct Decision

- Instead of sharing the data, Oti should explain to Kevo that doing so would be unethical and offer to help in some other appropriate way.
- Adhering to ethical principles may sometimes mean disappointing friends or foregoing potential advantages.
- However, following **professional ethics** ensures Oti acts **legally and morally**.
- It maintains his integrity and fulfills his obligations as a computing professional.

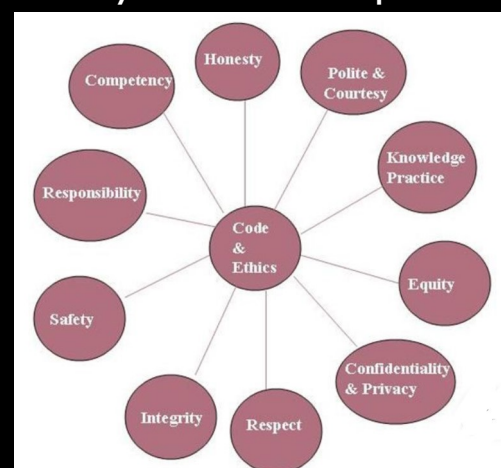
Professional Ethics

- The **moral principles and values** that guide the work and behaviour of professionals in their occupational fields.
- Involves reflecting on **the moral issues** that arise in one's **professional life** and determining the right way to act.

Professional Ethics

- These ethical considerations are essential for promoting **responsible** and **accountable conduct** in the tech industry.
- In computing, professional ethics is crucial as we have special responsibilities given the impact of computing on society.
- Unethical actions can result in harm.
 - Following ethics leads to fair, safe and moral outcomes.

Key Ethical Principles



Key Ethical Principles

- ❑ Honesty and Integrity
 - ❑ Being truthful, sincere, and straightforward in all professional dealings
 - ❑ e.g. transparency in communication and reporting.
 - ❑ Not lying, cheating, or stealing.
- ❑ Objectivity
 - ❑ Basing professional decisions on objective criteria.
 - ❑ Not emotions, personal values, or biases.

Key Ethical Principles

- ❑ Confidentiality
 - ❑ Protecting sensitive company or client information.
 - ❑ Not disclosing confidential data.
- ❑ Competence
 - ❑ Maintaining expertise and performing duties diligently, reliably, and safely.
 - ❑ Keeping skills up-to-date.
 - ❑ Professional Development: committing to ongoing learning and professional development to stay current in a rapidly evolving field.

Key Ethical Principles

- ❑ Accountability
 - ❑ Taking responsibility for one's actions and decisions.
 - ❑ especially in cases of technological failures or ethical dilemmas.
 - ❑ Admitting mistakes and failures.
- ❑ Respect for Others
 - ❑ Treating colleagues, clients, and all people with respect.
 - ❑ Not discriminating.
 - ❑ Ensuring fair treatment in technology development, use, and access.

Key Issues in Computing Ethics

- ❑ Privacy and Security/Data Protection
 - ❑ Respecting individuals' privacy rights
 - ❑ Secure handling of (esp sensitive) personal user data .
 - ❑ Securing computer systems, networks, and data against unauthorised access.
 - ❑ protect against cyber threats and breaches.
- ❑ Intellectual Property
 - ❑ Respecting intellectual property rights, including copyrights, patents and trade marks.
 - ❑ Not plagiarising or pirating software.

Key Issues in Computing Ethics

- ❑ Free Speech
 - ❑ Allowing free speech while preventing harm.
 - ❑ Filtering certain prohibited content.
- ❑ Automation and Bias
 - ❑ Ensuring AI systems are transparent, fair and unbiased.
- ❑ Digital Divide
 - ❑ Promoting equal access to technology across economic and social divides.

Key Issues in Computing Ethics

- ❑ Social Responsibility
 - ❑ considering the broader societal impacts of technology
 - ❑ striving to contribute positively to society.
- ❑ Environmental Responsibility
 - ❑ Minimising the environmental impact of technology
 - ❑ e.g., energy consumption and electronic waste.

Key Issues in Computing Ethics

- ❑ Ethical Decision Making
- ❑ Employing ethical decision-making frameworks to navigate complex ethical dilemmas and conflicts of interest.
- ❑ Popular Frameworks:
 - ❑ Utilitarianism
 - ❑ Deontological Ethics
 - ❑ Virtue Ethics
 - ❑ Rights-Based Ethics ...

Key Issues in Computing Ethics

- ❑ Rights-based ethics
 - ❑ based on the idea of **individual rights**
 - ❑ asserts that individuals possess certain fundamental rights that must be respected.
 - ❑ When facing an ethical dilemma, this framework requires considering the rights of all parties involved and making choices that do not infringe upon those rights.

Practical Strategies

- ❑ Risk-benefit analysis
 - ❑ Weighing the risks and benefits of actions.
- ❑ Whistleblowing policy
 - ❑ Reporting unethical conduct through proper channels.
- ❑ Ethics training
 - ❑ Taking courses on ethics and human values.
- ❑ Discuss dilemmas
 - ❑ Consulting others when facing an ethical predicament.
- ❑ Applying codes of ethics
 - ❑ Following industry codes of conduct ...

Codes Of Ethics

Professional Bodies

- ❑ A professional body is a formal group that oversees an area of an industry.
- ❑ Its purpose is:
 - ❑ To promote study and practice of the nominated area and to advance knowledge for the public benefit
 - ❑ To accredit individuals for their knowledge, learning and experience...

Professional Body Purpose (cont...)

- ❑ To define standards of conduct
- ❑ To advise the government and represent the profession
- ❑ To debate important topics
- ❑ To set standards for education and training
- ❑ To provide the opportunity for networking amongst its members

Professional Body Advantages

377

- Ability to share expertise
- Provides access to up to date information
- Legal protection for members
- Standardisation of qualifications
- Provision of periodicals/publications
- Holding of conferences and training

Professional Codes of Ethics

378

- Many professions have established **professional societies**.
- These have in turn adopted **codes of ethics/conduct**.
- These codes define and motivate **professional and ethical behaviour** by its members.

Professional Codes of Ethics

379

- The computing profession also has professional societies.
- Locally we have the Computer Society of Kenya.
 - Its members are expected to operate within the CSK Professional Code of Ethics and practice.

Professional Codes of Ethics

380

- Internationally we have several, with the two largest ones being:
 - The Association for Computing Machinery (ACM);
 - The Institute for Electrical and Electronics Engineers – Computer Society (IEEE-CS).
- We also have CompTIA IT Pro and Student Membership (formerly known as AITP).
- These US based organisations (with international reach) have also adopted **professional codes of ethics**.

IEEE-CS/ACM Software Engineering Code of Ethics and Professional Practice

- Established by the IEEE (Institute of Electrical and Electronics Engineers)
- A set of professional guidelines and codes of ethics for computer professionals.
- Provide ethical standards and principles for individuals and organisations in the field of computer science and software engineering.
 - they give us a framework for responsible and ethical behaviour and professional conduct.

IEEE-CS/ACM Software Engineering Code of Ethics and Professional Practice

- Emphasise the importance of
 - NOT ONLY **technical excellence** but
 - ALSO **ethical responsibility** and consideration for the broader societal impact of technology.
- When we adhere to these guidelines
 - we build trust
 - ensure the responsible development of technology, and
 - contribute positively to society.

Historical Context and Development

- Its development can be traced back to the early years of the software engineering profession.
- In the 1960s and 1970s, software engineering began to emerge as a distinct profession.
- With the growing importance of software in various industries, there was a need to establish ethical standards for practitioners.

Historical Context and Development

- This started with the formation of various professional organisations and associations.
- In 1999, the IEEE Computer Society (IEEE-CS) and the Association for Computing Machinery (ACM) collaborated to create a unified code of ethics.
- It was specifically tailored to software engineering.
- resulted in the "IEEE-CS/ACM Software Engineering Code of Ethics and Professional Practice."

The Principles

1. Public Interest
2. Client and Employer
3. Product
4. Judgment
5. Management
6. Professional Development
7. Colleagues
8. Society
9. Self

The Principles

- **Public Interest (Principle 1):** "Software engineers shall act in the best interests of the public."
- Computer professionals are encouraged to act in ways that serve the public interest.
- Includes ensuring societal safety and well-being.
- Ensure your work benefits society and does not harm individuals or communities.
 - Example: you discovers a critical safety flaw in autonomous vehicle software.
 - You must report it to protect public safety, even if it means revealing proprietary information.

The Principles

- **Client and Employer (Principle 2):** "Software engineers shall act in a manner that is in the best interests of their client and employer."
- Professionals should be loyal to their clients and employers, but
- they should also maintain integrity and avoid conflicts of interest ...

The Principles

- E.g., a software engineer working for a tech company must balance the interests of the customer with those of the company when handling a software defect that affects customers.
- Strive for accurate and honest reporting of software development progress and costs.
- Avoid misleading clients or employers.

The Principles

- ❑ **Product (Principle 3):** "Software engineers shall ensure that their products and related modifications meet the highest professional standards possible."
 - ❑ Ensure the products and systems you develop are reliable and of high quality.
 - ❑ Prioritise the best interests of the end-users.
 - ❑ E.g.: A software development team responsible for creating a medical records system must adhere to strict quality and security standards to protect patient data.

The Principles

- ❑ **Judgment (Principle 4):** "Software engineers shall maintain integrity and independence in their professional judgment."
 - ❑ Make informed and impartial judgments based on available data, without bias or prejudice.
 - ❑ E.g.: you may be asked to manipulate data to favour a particular outcome in a financial analysis tool you are building.
 - ❑ Upholding professional integrity and say NO.

The Principles

- ❑ **Management (Principle 5):** "Software engineers shall be fair to and supportive of their colleagues."
 - ❑ Foster a positive and collaborative work environment.
 - ❑ Treat colleagues with respect and support their professional development.
 - ❑ E.g.: a senior software engineer helps a junior colleague improve their coding skills

The Principles

- ❑ **Professional Development (Principle 6):** "Software engineers shall advance the integrity and reputation of the profession consistent with the public interest."
 - ❑ Continuous learning and development.
 - ❑ Continuously update skills and knowledge to stay current in the field.
 - ❑ E.g.: participate in industry conferences and share research findings to contribute to the advancement of the profession.
 - ❑ Support the professional growth of colleagues and subordinates.

The Principles

- ❑ **Colleagues (Principle 7):** "Software engineers shall moderate the interests of the software engineer, the employer, the client, and the users with the public interest."
 - ❑ Prioritise fairness and ethical considerations.
 - ❑ E.g., a software engineer faces a conflict of interest between fulfilling the demands of their employer and addressing the concerns of end-users to ensure a safe product.

The Principles

- ❑ **Society (Principle 8):** "Software engineers shall consider issues of privacy and the security of data."
 - ❑ Act to minimise the harmful impacts of software on society
 - e.g., address issues of discrimination, security, and privacy.
 - E.g.: A software development team working on a mobile app for healthcare must prioritise data privacy and security to protect patient information.

The Principles

- ❑ **Self (Principle 9):** "Software engineers shall be committed to making the analysis, specification, design, development, testing, and maintenance of software a beneficial and respected profession."
- ❑ Hold yourself accountable for ethical behaviour and decisions.
- ❑ Adhere to the highest standards of honesty and integrity.
 - ❑ E.g.: actively seek professional development opportunities, such as certifications, to enhance your skills and contribute to the profession's respectability.

Professional Ethics

- ❑ Professional ethics in computing guides ethical behaviour in areas such as
 - ❑ software development,
 - ❑ data handling,
 - ❑ cybersecurity, and
 - ❑ the responsible use of AI.

Professional Ethics

- ❑ Adhering to ethical principles is crucial for:
 - ❑ building trust
 - ❑ fostering responsible innovation
 - ❑ ensuring the positive impact of technology on society.

Why Ethical Behaviour Is Crucial in the Tech Industry

- ❑ Our codes of ethics **guide ethical decision-making and behaviour** in our rapidly evolving and influential field.
- ❑ **Ethical behaviour** is foundational to the tech industry's responsible development and use of technology.
 - ❑ it helps shape the industry's impact on individuals, society, and the world at large ...

Why Ethical Behaviour Is Crucial in the Tech Industry

- ❑ Protection of User Rights
 - ❑ Ethical behaviour safeguards users' rights, including privacy, security, and freedom from discrimination.
 - ❑ Users trust technology companies and professionals to safeguard their data and respect their digital rights.
- ❑ Trust and Reputation
 - ❑ Trust is a foundational element of successful **technology adoption**.
 - ❑ Ethical behaviour is essential for maintaining a positive reputation.
 - ❑ It builds trust with customers, clients, and the public.

Why Ethical Behaviour Is Crucial in the Tech Industry

- ❑ Legal Compliance
 - ❑ Ethical behaviour aligns with legal requirements and regulations.
 - ❑ Helps organisations avoid legal pitfalls, regulatory fines, and damage to their business due to unethical practices.
 - ❑ cf recently discussed case study on Kenya's ODPC actions.
- ❑ Innovation with Responsibility
 - ❑ Ethical tech professionals are more likely to innovate responsibly.
 - ❑ We consider the potential societal impacts of technology and take steps to mitigate harm and maximise benefits.

Why Ethical Behaviour Is Crucial in the Tech Industry

- Consumer Confidence
 - Consumer confidence in technology products and services is enhanced.
 - When users believe that their data and interests are protected, they are more likely to engage with and adopt new technologies.
- Global Impact
 - Technology has a global reach, and its ethical implications transcend borders.
 - Ethical behaviour in the tech industry contributes to global stability and cooperation in addressing cross-border issues such as cybersecurity and data privacy.

Why Ethical Behaviour Is Crucial in the Tech Industry

- Social and Environmental Responsibility
 - Ethical tech practices consider the broader social and environmental impacts of technology.
 - including reducing environmental footprints, promoting diversity and inclusion, and addressing societal challenges.
- Ethical Leadership
 - Ethical behaviour by tech leaders sets a positive example for the entire industry.
 - Encourages a culture of ethics and integrity throughout organisations and the broader tech community.

Why Ethical Behaviour Is Crucial in the Tech Industry

- Protection Against Misuse
 - Ethical guidelines help prevent the misuse of technology for harmful purposes
 - cyberattacks, surveillance, or the spread of disinformation.
- Long-Term Sustainability
 - Ethical behaviour contributes to the long-term sustainability of the tech industry.
 - Companies and professionals that prioritise ethics are more likely to endure and adapt to changing societal expectations.

Application of Ethical Codes in Real-World Scenarios

Case Study 2: Equifax

Equifax Data Breach (2017)

- One of the largest and most notable cybersecurity incidents in recent history.
- Occurred in 2017 when Equifax, one of the major credit reporting agencies in the United States, suffered a massive data breach that exposed sensitive personal information of approximately 147 million consumers.
- The breach included names, Social Security numbers, birth dates, addresses, and in some cases, even drivers' license numbers.
- The breach was attributed to a vulnerability in Equifax's website software, which the company failed to patch in a timely manner.
- Cybercriminals exploited this vulnerability to gain unauthorised access to Equifax's systems, where they were able to extract and steal vast amounts of personal data.

Equifax Data Breach (2017) vs the IEEE-CS/ACM Code of Ethics Principles

- Protecting Privacy
 - The breach of personal information at Equifax was a direct violation of the IEEE-CS/ACM Code of Ethics' principle of respecting and protecting individuals' privacy.
 - The company failed to adequately safeguard sensitive data, leading to a massive privacy breach affecting millions of individuals.

Equifax Data Breach (2017) vs the IEEE-CS/ACM Code of Ethics Principles

- ❑ Avoiding Harm
- ❑ Equifax's failure to secure its systems resulted in substantial harm to consumers.
 - ❑ The breach resulted in significant harm to individuals whose data was exposed.
 - ❑ potential for identity theft, financial fraud, and other negative consequences.

Equifax Data Breach (2017) vs the IEEE-CS/ACM Code of Ethics Principles

- ❑ Professional Competence:
 - ❑ It is our responsibility to maintain our competence and knowledge in our respective fields.
 - ❑ The Equifax breach raises questions about the professional competence of the company's IT and security teams.
 - ❑ The failure to promptly patch a known vulnerability suggests a lack of professional competence in cybersecurity practices.

Equifax Data Breach (2017) vs the IEEE-CS/ACM Code of Ethics Principles

- ❑ Honesty and Integrity
 - ❑ Equifax faced criticism for its handling of the breach, including delays in disclosing the incident to the public.
 - ❑ Timely and honest communication is crucial when a data breach occurs.
 - ❑ Any attempts to downplay or hide the severity of the breach can be seen as a breach of honesty and integrity.

Equifax Data Breach (2017) vs the IEEE-CS/ACM Code of Ethics Principles

- ❑ Responsible Computing
 - ❑ Equifax failed to patch a known vulnerability in a timely manner.
 - ❑ This demonstrates a lack of responsibility in ensuring the security of their systems and the protection of customer data.

Equifax Data Breach (2017) vs the IEEE-CS/ACM Code of Ethics Principles

- ❑ An excellent example of how violating the IEEE-CS/ACM Code of Ethics principles can lead to significant harm, privacy breaches, and reputational damage.
- ❑ Underscores the importance of
 - ❑ ethical considerations in technology
 - ❑ the responsibilities of organisations to protect sensitive data and act transparently and responsibly in the face of cybersecurity incidents.

Case Study 3

Ethical Hacking and Responsible Disclosure

Ethical Hacking, Responsible Disclosure, and Bug Bounty Programs

- ❑ **Ethical hacking**, aka penetration testing or white-hat hacking, involves **authorised** individuals or cybersecurity experts intentionally attempting to compromise computer systems, networks, or applications to identify vulnerabilities before malicious hackers can exploit them.
- ❑ **Responsible disclosure programs** provide a structured approach for reporting and addressing these vulnerabilities.
- ❑ **Bug bounty programs** offer financial rewards as incentives for ethical hackers to find and report vulnerabilities.
- ❑ All 3 are integral to modern cybersecurity practices.

Example

- ❑ A large technology company with a global presence runs a bug bounty program to identify and address security vulnerabilities in its software and services.

Example

- ❑ **Ethical Hacking**
 - ❑ Ethical hackers from around the world participate in the bug bounty program.
 - ❑ They actively probe the company's software and systems, searching for vulnerabilities that could potentially be exploited by malicious actors.
 - ❑ These ethical hackers use their expertise to test the company's security measures, identify weaknesses, and report their findings.

Example

- ❑ **Responsible Disclosure**
 - ❑ When ethical hackers discover vulnerabilities, they follow a responsible disclosure process outlined by the bug bounty program ...

Example

- ❑ This process typically involves:
 - ❑ Reporting the vulnerability to the company's designated security team through a secure channel.
 - ❑ Providing detailed information about the vulnerability, including how it was discovered and potential risks.
 - ❑ Allowing the company a reasonable amount of time to verify and address the vulnerability before disclosing it publicly.
 - ❑ Coordinating with the company to ensure that the issue is patched and resolved.

Example

- ❑ **Bug Bounty Rewards**
 - ❑ In return for their efforts and responsible disclosure, the company offers monetary rewards to ethical hackers who discover and report valid vulnerabilities.
 - ❑ The amount of the reward varies depending on the severity of the vulnerability and its potential impact on the company and its users.

Ethical Hacking, Responsible Disclosure, and Bug Bounty Programs vs the IEEE-CS/ACM Code of Ethics Principles

- Protecting Privacy
 - Ethical hacking, responsible disclosure, and bug bounty programs align with the principle of protecting privacy.
 - They aim to identify and mitigate vulnerabilities and weaknesses to prevent unauthorised access and data breaches.
 - Ultimately safeguarding individuals' privacy.

The 3 vs the IEEE-CS/ACM Code of Ethics Principles

- Avoiding Harm
 - Ethical hackers work to identify and mitigate potential harm by identifying vulnerabilities before malicious actors can exploit them.
 - Responsible disclosure ensures that vulnerabilities are promptly reported to organisations
 - This minimises the risk of harm to users.

The 3 vs the IEEE-CS/ACM Code of Ethics Principles

- Professional Competence
 - Ethical hackers must possess a high level of professional competence and expertise.
 - Their work directly impacts the security and integrity of systems and data.
 - They are thus expected to stay current with the latest security trends, tools, and techniques
 - in order to stay ahead of emerging threats and vulnerabilities.

The 3 vs the IEEE-CS/ACM Code of Ethics Principles

- Honesty and Integrity
 - Ethical hackers are bound by principles of honesty and integrity.
 - They are granted permission to test systems, but they must do so with transparency and honesty.
 - They must follow a strict code of conduct and not engage in any malicious activities.
 - they report vulnerabilities to organisations without malicious intent.

The 3 vs the IEEE-CS/ACM Code of Ethics Principles

- Responsible Computing
 - is promoted by ethical hacking, responsible disclosure, and bug bounty programs.
 - They proactively identify and address security vulnerabilities, contributing to safer and more secure digital environments.
 - Responsible disclosure emphasises responsible communication and cooperation between security researchers and organisations to patch vulnerabilities without causing harm or disruption.

The 3 vs the IEEE-CS/ACM Code of Ethics Principles

- Legal and Regulatory Compliance
 - The 3 must operate within the bounds of legal and regulatory frameworks.
 - They must ensure that their activities comply with applicable laws, contracts, and agreements.

The 3 vs the IEEE-CS/ACM Code of Ethics Principles

- ❑ Social Responsibility
 - ❑ The 3 contribute to a safer and more secure digital environment.
 - ❑ by identifying vulnerabilities, which, if left unaddressed, could lead to breaches affecting individuals and organisations.

Bug Bounty Programs: Additional Considerations

- ❑ These provide incentives for ethical hacking and responsible disclosure.
 - ❑ ethical hackers contribute to improved cybersecurity while adhering to ethical and legal guidelines.
- ❑ While they align with ethical principles, bug bounty programs introduce additional considerations ...

Bug Bounty Programs: Additional Considerations

- ❑ Fair Compensation
 - ❑ They must offer fair and reasonable compensation for discovered vulnerabilities.
- ❑ Ethical hackers should be rewarded in a way that reflects the severity and impact of the reported issue.

Bug Bounty Programs: Additional Considerations

- ❑ Transparency
 - ❑ They should operate transparently, with clear guidelines for ethical hackers regarding:
 - ❑ what is in scope
 - ❑ the rules of engagement
 - ❑ the process for reporting vulnerabilities.

Bug Bounty Programs: Additional Considerations

- ❑ Legal Protections
 - ❑ Participating ethical hackers should be provided with legal protections to prevent any legal action against them for their efforts.

Case Study 4

Professional Development and Social Responsibility

Professional Development and Social Responsibility

- **Professional development**
 - continuous learning
 - skill improvement
 - pursuit of knowledge
- to stay current with evolving technologies and best practices.
- **Social responsibility**
 - contributing to the betterment of society and the technology community.

Professional Development and Social Responsibility

- Active participation in open-source projects and knowledge sharing aligns with both of these principles.
- Consider a software engineer who actively participates in open-source projects related to cybersecurity.
- They contribute code, write documentation, and collaborate with a global community of developers to improve security tools.
- They also create educational materials and tutorials to help others understand cybersecurity concepts.

Professional Development vs the IEEE-CS/ACM Code of Ethics Principles

- **Enhance Competence**
 - Engaging in open-source projects allows them to enhance their competence by working on real-world software development challenges.
 - They acquire new skills, gain experience, and learn from collaborators.
- **Maintain Competence:**
 - Continuous involvement in open source keeps them up-to-date with the latest technologies and industry trends.

Social Responsibility vs the IEEE-CS/ACM Code of Ethics Principles

- **Contribute to Society**
 - Open-source software benefits users worldwide by providing free and accessible solutions to common problems.
- **Avoid Harm**
 - Responsible involvement in open source includes adhering to ethical standards and ensuring that contributed code and knowledge do not cause harm or compromise user security and privacy.

Social Responsibility vs the IEEE-CS/ACM Code of Ethics Principles

- **Knowledge Sharing**
 - Software engineers who share their expertise through documentation, tutorials, or mentorship help others learn and grow in the field.
- **Public Good**
 - Open-source projects provide essential software tools, educational resources, and infrastructure for communities, businesses, and governments.

Intellectual Property (IP)

&

IP Rights (IPR)

Should Property be Protected?

- Two separate theories provide the rationale for granting property rights:
 1. Property rights are a type of “**Natural Rights**”.
 2. Property rights are “**Social Contracts**”.

Should Property be Protected?

- Property rights are **natural rights** that ...
 - ought to be granted to individuals ...
 - for the products resulting from the labour expended in producing...
 - an artistic work or a practical invention.

Should Property be Protected?

- Property rights are **social contracts** designed to encourage creators and inventors **to better serve society** by bringing forth their artistic works and practical inventions into the marketplace.

Should Property be Protected?

- According to De Geoge, these two theories are also known as the **Standard Argument** (SA):
 - **Fairness/Justice**
 - Those who spend time, money, and resources in developing a product or expression of an idea deserve the chance to receive compensation.
 - **Utilitarian**
 - Society benefits from new products.
 - The best way to encourage the research and development of new products is by ensuring the opportunity to recoup their investment and to make a profit.

Should Property be Protected?

- **Consequentialist Theories** treat property rights as good as they lead to good consequences.
- Actually, both Locke’s **Natural Rights** and Bentham’s **Utilitarian** perspectives justify **monopolies** to encourage innovations that ultimately benefit the larger society ...
 - (cf. references)

Should Property be Protected?

- Their arguments are based on two premises
 1. monopolies create an ecosystem of innovations and creations
 2. such instruments are tools to benefit the public at large.

Should Property Be Protected?

448

- Let's take a closer look at these two theories (Natural Rights & Utilitarianism)

449

Property Rights Justified

- The Labour Theory of Property
- The Utilitarian Theory of Property

Should Property be Protected?

450

- Traditional theoretical foundations for property rights are often broadly grouped under
 - The Natural Rights theory of property
 - The Utilitarian theory of property

Should Property be Protected?

451

- **Natural Rights Theories:**
 - Derived from John Locke's 17th century **Labour theory**.
 - States that a person has a **natural right** to what they produce.

Locke's Theory of Appropriation

- Nature was created for all to share; it is a common.
- We each own our body, and the labour it produces.
- Mixing labour with the common yields a valid property claim.
 - if I put some labour into some common, then I have a claim to that common.
- Subject to caveats and provisos; not an absolute claim ...

Locke's Theory of Appropriation

- He did place some restrictions on the right to appropriation e.g.:
 - individuals have a natural right to acquire and possess property through their labour, but **The Lockean proviso** states that there had to be "enough and as good left in common for others".
 - implies that one can appropriate property from the common resources as long as there is enough and of similar quality left for others to use.

Locke's Theory of Appropriation

- He stated that labour is far from an absolute claim to title:
- "He that had as good left for his improvement as was already taken up needed not complain, ought not to meddle with what was already improved by another's labour; if he did it is clear he desired the benefit of another's pains . . ."

-- 2nd Treatise, ¶ 33

Locke's Theory of Appropriation

- Can be applied to software.
 - If I copy your software I'm stealing your labour.
 - I've made you lose the capacity to sell (and make money from) your creation.

Should Property be Protected?

- Locke argued that, generally, if you mix your labour with something then you have a legitimate claim to it.
- Weakness: why should we gain what we mix our labour with?
- Why not lose our labour?
- E.g. according to John Weckert (1996):
 - "If I poured a can of tomato juice, which I owned, into the sea, clearly I would not thereby own the sea. I would merely become juice less."

Utilitarian theory

The Utilitarian Theory of Property

- Granting property rights will maximise the good for the greatest number of people in a given society.
- Bentham's utilitarian moral philosophy or ethics = "the art of directing men's action to the production of the greatest possible quantity of happiness, on the part of those whose interest is in view."
- John Stuart Mill: the moral worth of actions is to be judged in terms of the consequences of those actions.

The utilitarian perspective

- "The greatest good for the greatest number"
- "Rights" follow only from **calculations of collective welfare**
- "Natural rights" are useless – Jeremy Bentham

466 Intellectual Property (IP)

INTELLECTUAL PROPERTY (IP)

467

- Intellectual property refers to creations of the mind such as inventions, designs, music, literary and artistic works, and symbols or names used in commerce.

INTELLECTUAL PROPERTY (IP)

468

- Refers to the results of intellectual activity in the industrial, scientific, literary or artistic fields.
- It is **intangible** property created by individuals or corporations.

INTELLECTUAL PROPERTY (IP)

469

- Intangible property arising from human intellect **that can only be protected upon expression**.
- Like other property, can be owned, administered by states, sold (assigned), leased (licensed), developed (exploited) and is usually enforceable by the law.

Intellectual Property Protection

470

- Legal, economics and management scholars have articulated legal doctrines that serve as the theoretical foundations for IP laws.

Moral Intuitions vis-à-vis IP Protection

1. The Scholar
2. The Entrepreneur
3. The Consumer
4. The Society

Moral Intuitions vis-à-vis IP Protection

- **The Scholar**
- Ideas should not be restricted.
- Only good can come from sharing ideas and challenging other ideas.
- However, it is NOT right to claim someone else's idea as yours.
- Always attribute correctly.

Moral Intuitions vis-à-vis IP Protection

- **The Entrepreneur**
- In order to make profits, businesses use resources in
 - product R&D,
 - production, and
 - product marketing.
- If you copy their product you deny them their just returns.

Moral Intuitions vis-à-vis IP Protection

- **The Consumer**
- What you as a consumer buy is yours to use as you please ...
- ... as long as you do not violate the Entrepreneur intuition.

Moral Intuitions vis-à-vis IP Protection

- **The Society**
- Basically, IP is social.
- It should be used for the common good.
- What if the common good and individual claims to IP clash?
- Appeals to the common good win.

The Need for IP Protection An Example Case

476

- Say it takes you quite some time and a lot of effort to come up with the capital required for your start-up.
- After all that, you use your time, knowledge and effort to develop some fantastic software.
- When you put it into the market it takes more time and effort to become popular but after a couple of years it picks up.

The Need for IP Protection An Example Case

477

- You recover 10% of the start-up capital and other expenses but two things happen in the 3rd year:
 - Because your software is so fantastic everyone wants it (and gets it) but almost no one is paying you for their copy.
 - A pirate copies and modifies your software and sells it at much cheaper price. After all, their development costs are minimal.
- Despite your best efforts, your business collapses in the 4th year.

The Need for IP Protection

- 478
- We can all agree that something seems unfair here.
- **Q:**
- What should we do to prevent this?
- **One (legal) answer:**
- Allow you to have LEGAL exclusive rights to your software.
- Then you can deal with the pirates via the law.

The Need for IP Protection

- 479
- **The Goal of IP Law**
- To encourage the development of **ideas** and **devices ...**
- by giving the originator **exclusive** rights ...
- to obtain **remuneration** for the use of the idea or device ...
- for some **period of time.**

The Need for IP Protection

- 480
- Software **is** IP.
- The free flow and use of **digital** information has an open border.
 - Difficult to control copyrights, authorship, other IPR.
- There is a need for **standard procedures, regulations and laws.**
- These must be designed to be **implemented in technical solutions.**

The Need for IP Protection

- 481
- Only then can we control the trade, storage and use of individuals', communities', state organisations' and other bodies' IP.
- For example:
 - **A copyright law** protects literary and artistic works
 - **A patent law** protects inventions
 - **A trademark law** protects the rights of businesses to their **identity**
 - e.g. a company logo

The Need for IP Protection

- 482
- All these concepts have been around much longer than the computer.
- However, their **digital representation** has raised various legal issues.

The Need for IP Protection

- 483
- Today's information systems severely challenge existing law and social practices that protect private IP.
- Digital information is easily copied or distributed via networks.

484

IPR

Challenges in the 21st Century

IPR: Challenges

485

- ❑ Contemporary ITs, especially software, pose severe challenges to existing IP regimes.
- ❑ They create significant ethical, social, and political issues.
- ❑ Digital media differ from physical media
 - ❑ E.g. books, periodicals, CDs, and newspapers ...

IPR: Challenges

486

- ❑ Digital media are:
 - ❑ easy to replicate;
 - ❑ easy to transmit;
 - ❑ easy to alter;
 - ❑ compact (easy to steal)

IPR: Challenges

487

- ❑ It is also difficult to classify a software work as a program, book, or even music;
 - ❑ SW code can be **copyrighted** like a book, but can also include audio/visual components resembling music or art.
 - ❑ SW often combines various media forms: text, images, audio, video, and interactive elements. E.g: an educational app might include text-based content, images, and interactive quizzes.
 - ❑ e-books often include multimedia content
 - ❑ SW can be used to create generative art or algorithmic music - the output is generated through algorithms and not necessarily the direct result of human creativity. This blurs the line between software and traditional artistic forms.

IPR: Challenges

488

- ❑ It is also difficult to establish SW's uniqueness.
 - ❑ Can be extremely complex, with millions of lines of code; challenging to analyse all this code thoroughly to determine if it's entirely unique.
 - ❑ Is inherently **abstract**, consisting of lines of code and data that are not physical objects; difficult to assess its uniqueness compared to tangible, physical items.
 - ❑ Many SW programs **reuse** standard functions and code libraries thus certain parts of different programs may be similar or even identical.
 - ❑ Unrelated developers can **independently develop similar solutions** to common problems=>similar software even though there was no copying.
 - ❑ SW dev is often an iterative process where small changes are made over time; a program may **evolve gradually**, making it challenging to pinpoint when it became unique.

489

Legal Mechanisms To Protect Software

Legal Mechanisms To Protect Software

- ❑ Trade Secrecy
- ❑ Patents
- ❑ Copyright
- ❑ Trade Mark
- ❑ Registered Design
- ❑ Domain Name protection

Kenyan Laws Governing Intellectual Property

Kenya's Legislative Instruments

- ❑ Include:
 - ❑ Copyright Act No. 12 of 2001
 - ❑ Trade Marks Act Cap 506 (as last amended by the Trade Marks Act, 2002)
 - ❑ Industrial Property Act (IPA) No 3 of 2001
 - ❑ Anti-Counterfeit Act (2008)
 - ❑ The Geographical Indications Act
 - ❑ Seed and Plant Varieties Act, Cap 326

Legal Mechanisms To Protect Software

- ❑ Kenya has well-established laws to protect **intangible** property rights.
- ❑ We are part of various international agreements and organisations that promote the protection of intellectual property rights.
- ❑ The government encourages innovation and entrepreneurship through **legal provisions** that protect intellectual property rights (IPR).
- ❑ Any IP owner must register their original works or products with the relevant bodies to protect their rights.

1. The Copyright Act of Kenya

- ❑ Protects literary, musical, and artistic works from reproduction, communication to the public, and distribution without the owner's authorisation.
- ❑ Includes music, books, films, and software programs' protection.
- ❑ It's the owner's responsibility to register their work with the **Kenya Copyright Board**.

2. The Trademarks Act of Kenya

- ❑ Protects symbols, names, and logos used to identify goods and services from unauthorised use.
- ❑ Trademark registration and renewal are mandatory to prevent infringement.

3. The Industrial Property Act of Kenya

496

- ❑ Provides protection for
 - ❑ inventions,
 - ❑ designs, and
 - ❑ trade secrets.
- ❑ Establishes the **Kenya Industrial Property Institute** (KIPI) responsible for registration and renewal of patents, designs, and utility models.
- ❑ Prohibits the use, sale or importation of infringing products.

4. The Anti-Counterfeit Act

497

- ❑ Prohibits the manufacture, distribution or sale of counterfeit goods.
- ❑ Defines counterfeit products as replicas of genuine products without the owner's authorisation.
- ❑ Helps to protect businesses from losing profits and IPR infringement.

5. The Geographical Indications Act

498

- ❑ Protects products originating from specific regions from unauthorised use.
- ❑ It seeks to protect the IPR of producers of traditional products.
- ❑ It's mandatory to register geographical indications with KIPI.

IP Law

499

- ❑ IP is usually subjected to a variety of protections under three different legal traditions:
 - ❑ trade secrets,
 - ❑ copyright, and
 - ❑ patent law.

500 Trade Secrecy

Trade Secrecy

501

- ❑ Trade secrets **must**
 - ❑ have novelty
 - ❑ represent economic investment by claimant
 - ❑ have involved development effort
 - ❑ have been the subject of considerable effort to protect secrecy
- ❑ Mechanisms
 - ❑ non-disclosure clauses in contracts of employment
 - ❑ licence agreements

Trade Secrets

- 502 ☐ Any **intellectual work product** used for a business purpose can be classified as a trade secret...
 - ☐ Provided it is not based on information in the public domain.
- ☐ Examples of **intellectual work products**
 - ☐ a formula
 - ☐ a device
 - ☐ a pattern
 - ☐ a compilation of data
- ☐ used for a business purpose

Trade Secrets

- 503 ☐ Generally, trade secret laws grant a monopoly on the **ideas** behind a work product.
- ☐ **Software** that contains novel or unique elements, procedures, or compilations can be included as a trade secret.
- ☐ Trade secret law protects the **actual ideas** in a work product...
- ☐ ... NOT just their **manifestation**.

Trade Secrets

- 504 ☐ If you are a creator or owner claiming Trade Secrets protection, ensure you've bound your employees and customers to non-disclosure agreements (NDAs).
- ☐ You must do everything necessary to prevent the secret from falling into the public domain.

Trade Secrets

- 505 ☐ **Limitation**
- ☐ True, almost all complex software programs contain **unique** elements of some sort.
- ☐ However, it is difficult to prevent the **ideas** in the work from falling into the public domain when the software is widely distributed.

Trade Secrecy Limitations

- 506 ☐ Can't enforce employee confidentiality to extent of preventing **re-use** of ideas
 - ☐ E.g.: say you own a company that develops a browser whose UI is loved by its users.
 - ☐ You eventually sell the company and create another one.
 - ☐ Much to most of its users' displeasure, your former company changes the popular browser's UI.
 - ☐ You develop a browser who's UI is what most liked.

Trade Secrecy Limitations

- 507 ☐ Similarly, licensing agreements can't prevent users from exploiting experience with proprietary software to build 'a better mousetrap'
 - ☐ (create a better version of a widely used product).

Trade Secrecy Limitations

508

- ❑ Strong protection allows the owner to keep their idea & its manifestation out of the public realm ...
- ❑ ... but **once exploited, this is lost.**

Sources of an Obligation of Confidence

509

- ❑ Express contract
- ❑ Implied contractual obligations

Sources of an Obligation of Confidence

510

- ❑ Express contract
 - ❑ **Express terms** are those that have been specifically mentioned and agreed by both parties at the time the contract is made.

Sources of an Obligation of Confidence

511

- ❑ Implied contractual obligations
 - ❑ **Implied terms** are not expressly outlined in the contract but which legislation, and the courts, deem to be part of the contract.
 - ❑ Two main types of implied terms:
 - ❑ implied by statute
 - ❑ implied by the courts

Sources of an Obligation of Confidence

512

- ❑ **Express contract**
 - ❑ e.g.
 - ❑ Non Disclosure Agreement
 - ❑ Confidentiality Agreement
 - ❑ Can be oral or written (the latter is better for evidence)
- ❑ **Standard Exceptions**
 - ❑ "Black Box" agreement – user can use the device, but not take it apart (can apply to computers)

Sources of an Obligation of Confidence

513

- ❑ **Implied contractual**
 - ❑ May be used to supplement express terms
 - ❑ e.g. an **express** term against disclosure of confidential information ...
 - ❑ could be supplemented by an **implied** term prohibiting its use.

Obligation Of Confidence ...

- 514 ☐ An obligation of confidence is owed by **employees**;
- ☐ **During employment** – strict obligation of confidence
- ☐ **After employment** – can be bound **explicitly** or **implicitly**:
 - ☐ **Explicitly**: Covenant in restraint of trade
 - ☐ **Implicitly**: Obligation of good faith (fidelity)

Obligation Of Confidence ...

- 515 ☐ After employment:
- ☐ **Explicitly: Covenant in restraint of trade** (must be “**reasonable**”)
 - ☐ When courts are considering whether to enforce such a covenant they scrutinise it’s **reasonableness** (see the slides titled *Explicit Obligation of Confidence...Covenant in restraint of trade*)
 - ☐ The parties can agree to any express term as long as it’s legal.

Obligation Of Confidence ...

- 516 ☐ **Implicitly**: Obligation of good faith (fidelity) on the part of the **employee**
- ☐ **Implied by law** - they must avoid all **conflict of interest** situations.
 - ☐ When employed, they must therefore not use trade secrets or confidential info for their own benefit to the detriment of the employer.

Explicit Obligation of Confidence... Covenant in restraint of trade

- 518 ☐ **Restraint of trade:**
 - ☐ employers and employees can negotiate and agree to almost any express term in employment contracts.
 - ☐ However an employer’s ability to enforce a covenant in restraint of trade against an ex-employee is not so straightforward.
 - ☐ It’s quite difficult for employers to implement **restrictive trade clauses** (RTCs).

Explicit Obligation of Confidence... Covenant in restraint of trade

- 519 ☐ Kenya’s Employment and Labour Relations Court has held that RTCs
 - ☐ are constitutional and generally enforceable **if reasonable**.
 - ☐ must be balanced against the employee’s circumstances.
- ☐ RTCs must comply with the Contracts in Restraint of Trade Act (CRTA) - (Chapter 24, Laws of Kenya), to stand any chance of enforcement.

Obligation Of Confidence ... Contracts in Restraint of Trade Act (Cap 24)

- 520 ☐ A provision or covenant restraining one party from exercising any lawful profession, trade, business or occupation is not void
- ☐ However, the High Court shall have the power to declare the provision or covenant to be void if
 - ☐ the provision or covenant is not reasonable either in the interests of the parties; or
 - ☐ the provision or covenant is injurious to the public interest

Obligation Of Confidence ...

Contracts in Restraint of Trade Act (Cap 24)

521

- ❑ Considerations when ruling on Non-Compete clauses include
 - ❑ Reasonableness
 - ❑ Time
 - ❑ Scope of activities
 - ❑ Geographical coverage
 - ❑ Legitimate interest
 - ❑ Public Interest

Obligation Of Confidence ...

Contracts in Restraint of Trade Act (Cap 24)

522

- ❑ These are balanced against an **employee's right to employment ...**
- ❑ that has recently been prioritised over the **employer's right to protect its business interests.**

Obligation Of Confidence ...

Contracts in Restraint of Trade Act (Cap 24)

523

- ❑ **Case Law**
- ❑ ***Credit Reference Bureau Holdings Ltd vs Kunyiha (2017)***
- ❑ Steven Kunyiha, the former chief executive officer of Credit Reference Bureau Holdings Ltd (CRBH) was prohibited from
 - ❑ entering into employment with any competitor of CRBH for a period of 12 months after the termination of his employment ...
 - ❑ disclosing any confidential and proprietary business information to CRBH's competitors.

Obligation Of Confidence ...

Contracts in Restraint of Trade Act (Cap 24)

524

- ❑ Kunyiha got a job with a direct competitor of CRBH.
- ❑ The latter sought injunctive orders restraining him from taking up employment on the grounds that the competitor would gain
 - ❑ access to its confidential and proprietary business information and
 - ❑ an unfair advantage over CRBH in its business operations.
- ❑ The court declined CRBH's application.
- ❑ It referred to another case in which the court held that any damage that might be caused to the employer was secondary to the impact an injunction would have on the employee's ability to find another job.

Obligation Of Confidence ...

Contracts in Restraint of Trade Act (Cap 24)

525

- ❑ Held:
- ❑ "in a country like Kenya where unemployment is soaring every single day, subjecting the defendant to loss of employment on the basis of a restrictive clause would be unreasonable and not in the interest of either party. Indeed such an action would be contrary to public policy" as courts should not be seen to be unduly impeding upon a person's right to earn a living.
- ❑ A **reasonableness** test that the courts have laid down:
 - ❑ Subjecting the former employee to a period of unemployment with no guarantee of employment following this period would be unreasonable and against the public interest in the Kenyan context where unemployment is soaring.

Obligation Of Confidence ...

Contracts in Restraint of Trade Act (Cap 24)

526

- ❑ Also held:
- ❑ CRBH had failed to discharge the **burden of proof:**
 - ❑ The employer cannot reasonably restrain the experience and expertise gained from a particular employer without stunting the employees career.
 - ❑ The RTC must seek to restrain the employee's use of only that which is uniquely the employer's secret and not the employee's use of experience, knowledge or skill gained from working with the employer (i.e. which can be acquired by learning, experience or development in technology) ...

Obligation Of Confidence ...
Contracts in Restraint of Trade Act (Cap 24)

527

- ❑ CRBH had failed to demonstrate
 - ❑ the nature of the secrets or information to which Kuniya had gained access and
 - ❑ the manner in which he was likely to divulge or use the same in his new employment to the detriment of CRBH.
- ❑ Further, CRBH had not shown that Kuniya had in his possession classified information

Obligation Of Confidence ...
Contracts in Restraint of Trade Act (Cap 24)

528

- ❑ **Other Case Law**
- ❑ LG Electronics Africa Logistics FZE vs. Charles Kimari (2012)
 - ❑ *Restrictive clause is only unconstitutional if it does not meet the limits set by Section 2 of the Contracts in Restraint of Trade Act (Cap 24)*
- ❑ Bridge International Academies Limited versus Robert Kimani Kiarie (2017)
 - ❑ *The plaintiff had only made allegations without suitable proof, which were easily denied by the defendant.*

Obligation Of Confidence ...
Contracts in Restraint of Trade Act (Cap 24)

529

- ❑ How can the employer be helped?
- ❑ **Garden Leave**
- ❑ Consider including a garden leave clause alongside the restraint
- ❑ Garden leave describes the practice where an employee who has resigned or is dismissed with notice is instructed to stay away from work during the notice period, while still remaining on the payroll.
- ❑ More likely to be upheld as employee is receiving compensation
- ❑ Undeveloped Case Law in Kenya
- ❑ UK Case Law can give us ideas

Obligation Of Confidence ...
Contracts in Restraint of Trade Act (Cap 24)

530

- ❑ **More on Garden Leave:**
- ❑ The employee remains on the payroll for a period
 - ❑ (typically upto 6 months)
- ❑ but is not allowed to go to work or to commence any other employment.
- ❑ Usually implemented as the employee may have access to up-to-date information which could be beneficial to the employer's competitors
- ❑ so the employer ensures that by the time the employee is contractually free, he or she would have been out of the loop long enough to reduce this threat.

Obligation Of Confidence ...
Contracts in Restraint of Trade Act (Cap 24)

531

- ❑ A garden leave clause typically found in the contracts of senior employees to:
 - ❑ Stop an employee working for a competitor until their notice period has come to a close
 - ❑ Keep them away from confidential or sensitive company data and prevent them from misusing this data
 - ❑ Stop the employee from poaching customers or colleagues
 - ❑ Enable the successor to the role without worrying that the other employee will get in the way.

532

Patents

NB: Find out the process of obtaining the various means of protection in Kenya (visit <http://kipi.go.ke/>)

Patents Protection

533

- ❑ Knowledge is only useful if it contributes to development.
 - ❑ It must be **exploited** and **transferred**.
 - ❑ **Transfer** can only happen effectively through legal **protection and commercialisation** which require an **owner** and a **value**.
- ❑ **Patents** move beyond just the knowledge (**ideas**) to the thing (**commercialisation**).
- ❑ Innovation vs Invention:
 - ❑ Innovation is the process of translating an idea or invention into a good or services that creates value ...

Patents Protection

535

- ❑ A patent grants the owner an exclusive monopoly on the ideas behind an invention for 20 years.
- ❑ Its intent:
 - ❑ To ensure that inventors of new machines, devices, or methods receive the full financial and other rewards of their labour **yet still make widespread use of the invention possible**.
- ❑ How?
 - ❑ By providing detailed diagrams for those wishing to use the idea under license from the patent's owner.

Patents

536

- ❑ A patent protects inventions and encourage inventors to innovate.
- ❑ A patent gives to an inventor a legitimate **monopoly** in an invention.
 - ❑ This means that the inventor is given the exclusive right to use or exploit the invention for a defined period (20 years in Kenya).
- ❑ A grant of the right to exclude others from making, using, importing or selling one's invention without permission.
 - ❑ includes right to license others to make, use, or sell it

PATENTS

537

- ❑ Fill Kenya Industrial Property Institute (KIPI)'s form IP3 (*Application for a Patent*)
- ❑ A granted patent must be renewed every year after the 5th year for up to 20 years.

Patent Claims

538

- ❑ For an invention to be patentable it:
 1. **must fall within the category of permissible subject matter:**
 - ❑ "a process, machine, manufacture or composition of matter or ... an improvement thereof."

Patent Claims

539

2. Must have the following characteristics (i.e. it **must satisfy three tests**):
 - i. **Novelty** - It must be new (not used anywhere else)
 - ii. **Non-obviousness** - It must have an **inventive step** that is not obvious to someone with knowledge and experience in the subject
 - ❑ someone skilled in the field of invention sees it as an unexpected or surprising development
 - iii. **Utility/industrial applicability** - It should be capable of being made or used in some kind of industry; it must work/have a useful application (you can apply it in industry or agriculture)

Patent Claims

540

- ❑ All these (the 3 tests) are tested by KIPI (Kenya Industrial Property Institute).
- ❑ If your invention makes the cut, you can then have the rights to control who makes, uses, sells, offers to sell and/buy and/or imports the patented invention.
- ❑ NB for IP:
 - ❑ FCFS (ownership)
 - ❑ E.g., for patents: first inventor to file an application

Patent Claims

541

- ❑ Registering with KIPI = only local protection
- ❑ ARIPO - African Regional Intellectual Property Organisation
 - ❑ (do it through KIPI) - African countries
- ❑ WIPO - World Intellectual Property Organisation
 - ❑ If you want international protection you must go to KIPI first then WIPO.

What You Can't Patent

542

- ❑ It must not be:
 - ❑ a literary, dramatic, musical or artistic work
 - ❑ a way of performing a mental act, playing a game or doing business
 - ❑ the presentation of information, or some computer programs
 - ❑ an animal or plant variety
 - ❑ a method of medical treatment or diagnosis
 - ❑ against public policy or morality
 - ❑ a scientific or mathematical discovery, theory or method...

What You Can't Patent

543

- ❑ ***It must not be a scientific or mathematical discovery, theory or method ...***
- ❑ Say you make a new and useful scientific discovery that no one else has ever thought of.
- ❑ You cannot get a patent on it because **you did not actually create** the fact you discovered.
- ❑ That fact was always in existence, you were just the first to notice it.
- ❑ However, if you can come up with an invention that makes use of that fact, you can patent the invention.

Patents Protection

544

- ❑ **Advantage**
- ❑ It grants a monopoly on the underlying concepts and ideas of software.
- ❑ **Disadvantages**
- ❑ Proving non-obviousness, originality, and novelty is hard.
 - ❑ e.g., the work must reflect some special understanding and contribution.
- ❑ The amount of time it takes before receiving protection (sometime years).

557

Patenting Software

Summary

Patent principles

- Purpose is the advancement of the useful arts and sciences
 - not simply the right of inventors to reap rewards - a means not an end
- Foster inventions
- Promote disclosure of inventions
- Assure ideas in public domain remain free
- Improve economy and employment

Patents and Software

- Until 1980's, patent offices were reluctant to grant software patents for fear of granting ownership of mental processes
 - patent holder could require a licence to perform operations mentally
- More recently the focus is on the nature of mathematical algorithms
 - explicitly excluded as inappropriate subject matter

Patents and Software

- Although software functions by using algorithms and mathematics, it may be patentable if it produces some concrete and useful result.
- However, what cannot be patented is software whose only purpose is to perform mathematical operations.
- Not Patentable:
 - software that converts one set of numbers to another
- Patentable:
 - software that converts one set of numbers to another to make rubber ...

Patents and Software

- Initially, the US's Patent Office rejected **software** patents applications.
- Until the ***Diamond versus Diehr (1981)*** Supreme Court decision:
 - computer programs could be a part of a patentable process.
 - The plaintiff (Diehr) had applied for a patent on a process for curing synthetic rubber.
 - His machine could cure rubber aided by a computer using mathematical formulae.

Claiming a software patent

- Before putting to market, do ex(t/p)ensive patent search
 - If overlapping patents, secure licences
- Patent searches are unreliable as the classification system for software is poor
 - Easy to spend development £\$Ksh only to find a relevant claim has been filed
- Conclusion: patents do not serve interests of innovation in software

Read about relevant cases from <http://www.richardspatentlaw.com/faq/have-an-idea/what-do-you-think-about-software-patents/>

Further Reading

- Check out the following article titled **"Filing for a Patent Versus Keeping Your Invention a Trade Secret"**
- <https://hbr.org/2013/11/filing-for-a-patent-versus-keeping-your-invention-a-trade-secret>

564

COPYRIGHT PROTECTION

Copyright is a form of protection provided by the laws of a country to the authors of original works in the industrial, scientific, **literary** or artistic fields.

COPYRIGHT PROTECTION

565

- ❑ **Literary works** may include such things as written material, music, drama and paintings.
- ❑ The protection is available to **published or unpublished** works.
 - ❑ provided it meets the relevant legal criteria and requirements.
- ❑ Both **source code** and **object code** are taken to be literary works.
- ❑ Hence they are copyrightable.

Copyright Protection

566

- ❑ Copyright protects IP creators from having their work copied by others for any purpose.
- ❑ In Kenya, the duration is **the life of the author plus an additional 50 years** after the author's death.
- ❑ The **intent** behind copyright laws is to encourage creativity and authorship.
- ❑ Creative people receive financial and other benefits of their work.

Copyright Protection

567

- ❑ Many countries/nations have their own copyright laws.
- ❑ They also ratify international conventions and bilateral agreements on IPR.
- ❑ For **SW**, copyright laws allow the **buyer** to use the SW while the **creator** retains legal title.
- ❑ Copyright protects against copying of parts of, or the entire program.
- ❑ Damages and relief are awarded for infringement.

Copyright Protection

568

- ❑ **Disadvantage:**
- ❑ The underlying **ideas** behind a work are not protected, only their **manifestation** in a work.
- ❑ A competitor can use your software, understand how it works, and build new software that follows the same concepts without infringing on a copyright...

Copyright Protection

569

- ❑ “**Look and feel**” copyright infringement lawsuits are about differentiating between an idea and its expression.
 - ❑ E.g. in the early 1990s **Apple Computer sued Microsoft Corporation and Hewlett-Packard** for infringement of the expression of Apple's Macintosh interface.
- ❑ They claimed that the defendants copied the **expression** of overlapping windows.

Copyright Protection

570

- ❑ The defendants countered that the **idea** of overlapping windows can be **expressed** only in a single way ...
- ❑ Thus it was not protectable under the **merger doctrine** of copyright law:
 - ❑ When **ideas and their expression merge**, the expression cannot be copyrighted.

Copyright Protection

571

- ❑ In general, courts appear to be following the reasoning of the **Brown Bag Software vs. Symantec Corp (1989)** case.
 - ❑ The court found that similar concept, function, general functional features (e.g., drop-down menus), and colors are not protectable by copyright law.
 - ❑ In copyright law, **functional aspects** are not typically protected, whereas **creative expressions** can be.
 - ❑ In the Apple case, overlapping windows were held to be functional features rather than purely creative expressions.

COPYRIGHT PROTECTION

572

- ❑ Copyright is ...
- ❑ a form of ownership ...
- ❑ that excludes others,
- ❑ for a limited amount of time,
- ❑ from copying without permission.

COPYRIGHT PROTECTION

573

- ❑ You can NOT copyright an idea.
- ❑ Q: What, then, can you copyright?
- ❑ The **expression of an idea**.
- ❑ What is the difference?
- ❑ One way to look at it:
 - ❑ The idea is the **concept**, the expression is the **way it is realised**.
 - ❑ The expression would be the exact words in the work.

COPYRIGHT PROTECTION

574

- ❑ What is protected is the **fixation of an idea in a tangible medium of expression**,
- ❑ We can't protect the idea itself, or any processes or principles associated with it.
- ❑ The distinction is not always clear and is usually on a case by case basis.
- ❑ **Source and object codes** are copyrightable because they are **expressions of ideas**.

COPYRIGHT PROTECTION

575

- ❑ A problem arises here.
- ❑ It is very, very simple to make a whole new app by changing very little in an existing software.
- ❑ Think back to the case study of the fantastic software start-up that collapsed due to piracy.
- ❑ To what does the copyright apply?
 - ❑ The old version?
 - ❑ The parts of the new version with the old code?

COPYRIGHT PROTECTION

576

- In this case, this question arises even when you, the owner modifies the app.
- Should you reapply for copyright each time you add new pieces of code?
- Maybe viewing software as 'literary works' is over simplifying the issue ...

Is Software Literature?

577

Literature

- Doesn't change much.
- If I create a literary work similar to yours I can acquire protection for it if I did it independently and it is **literally different**. (cf. Whelan versus Jaslow.
- For literature to be useful, a user must be present

Software

- Constantly changing.
- If I independently develop software strikingly similar to yours, I may not be able to copyright it.
- Software behaviour is useful in itself, even with no users.

Case Law

578

- **Whelan versus Jaslow (1986) aka Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc**
- Whelan developed a program for Jaslow in Fortran.
- The agreement was that Whelan would own it.
- Jaslow then redid the program line by line in BASIC.
- Whelan sued.

Case Law

579

- Though Jaslow's program was *literally different* and maybe even a different expression of the same idea, the court found in favour of Whelan.
- They found comprehensive **non-literal similarity**.
 - It may not be a literal copy (of the text of the code), but the (more abstract) **structure, sequence and organisation** (SSO) were copied.
- **cf Lotus vs Borland (1996) Idea vs expression of an idea**
 - *Held: A computer menu command hierarchy is not copyrightable subject matter.*

Case Law

580

- **Franklin Computer Corp versus Apple (1984)**
- Apple had proprietary software that could only run on the Apple II.
- Franklin developed a clone, the Franklin ACE 1000 whose ROM and OS were indisputably copied from Apple (practically line by line).
 - The programs were in object code stored in ROM.
- He was found guilty of copyright infringement.

Case Law

581

- An appeals court held that:
 1. a computer program, whether in object code or source code, is a "literary work" and is protected from unauthorised copying
 2. a computer program in object code embedded in ROM chip is an appropriate subject of copyright;
 - Franklin had argued that
 - (1) Apple's software existed only in machine-readable form (not in printed form), and
 - (2) some of the software did not contain copyright notices.

Case Law

- 582
- An appeals court held that ... (cont):
 - 3. computer operating system programs are not per se precluded from copyright protection;
 - (first time a court had ruled that an OS was copyrightable)
 - 4. even without the presumption of irreparable harm generally applied to copyright infringement actions, Franklin copying key programs would irreparably harm Apple's investment and competitive position. This was enough to justify a preliminary **injunction**.
 - 5. Irreparable harm must be presumed in every copyright case.
 - (A lower court had found that Franklin's was too small a company to pose any serious threat to Apple but granting Apple a preliminary injunction would probably bankrupt Franklin.

COPYRIGHT PROTECTION

- 583
- Digital representation of IP has made it easier to infringe copyright, and policing of copyright infringement has become difficult.
 - The Internet is one area where this has become very difficult due to the number of people who are performing copying of IP.
 - One point of contention is **fair use** of copyrighted material that are copied for personal use, education or research and not for commercial purpose.

- 584
- Copying may be allowed in the licence e.g. for fair use and back-up purposes.
 - **Fair use:**
 - Teaching
 - Scholarly work/research
 - Criticisms or comments
 - News reporting
 - Some governmental purposes e.g.:
 - parliamentary/judiciary proceedings
 - commissions and statutory inquiries.

- 585
- Computer Software is considered as copyrightable material including freeware, shareware, and commercial software.
 - Only **public domain** and **open source software** fall outside the copyrighted restrictions.
 - When you buy software you are bound by the license agreement.
 - License agreements allow you to **use** the software and **not to modify, sell or give it away** as those rights belong to the copyright holder.

- 586
- Digital images like photographs, art-like cartoons or complex images are copyrighted material
 - but under **fair use** a downloaded image can be used as a screen saver
 - but you are not allowed to distribute or post it in your own web site.
 - **Plagiarism**
 - under the fair use practices you can include someone's work **as long as you identify the source**.

587

The Kenyan Copyright Act

The Kenyan Copyright Act of 2001

- ❑ Kenya has a robust intellectual property rights (IPR) legal framework.
- ❑ This framework primarily falls under copyright law, which is aimed at protecting the creativity of individuals, authors, and artists.
- ❑ The Kenyan Copyright Act of 2001 governs copyright law in the country.
- ❑ It takes a comprehensive approach to the protection of literary, artistic, musical, and other creative works.
- ❑ It outlines:
 - ❑ the rights of copyright owners
 - ❑ limitations on exclusive rights
 - ❑ remedies available to parties in cases of infringement.

The Kenyan Copyright Act of 2001 The Rights of Copyright Owners

- ❑ Protects original works of art, including music, broadcasts, films, photographs, and literary works.
- ❑ Gives exclusive rights to copyright owners to:
 - ❑ reproduce, distribute, display, and perform their work.
 - ❑ create a derivative work or adaptation of their work.

The Kenyan Copyright Act of 2001 Limitations On Exclusive Rights

- ❑ The Act defines the limitations on these exclusive rights e.g.:
 - ❑ the use of work for educational, scientific, and research purposes may be allowed in certain circumstances.
- ❑ However, such use must not infringe on the rights of the copyright owner.

The Kenyan Copyright Act of 2001 Remedies

- ❑ The Act outlines the remedies available to parties who are affected by copyright infringement.
- ❑ These remedies include civil and criminal action.
- ❑ In civil proceedings, a copyright owner can seek an injunction to stop an infringing party from continuing an action that infringes on their rights.
- ❑ They can also claim damages and seek an account of profits made by the infringing party.
- ❑ In criminal proceedings, an infringing party can face imprisonment and fines.

The Kenyan Copyright Act of 2001

- ❑ The Kenyan Copyright Act also outlines the role of collective management organisations (CMOs).
- ❑ These are registered under the Act and are responsible for **administering the licenses** for the use of copyrighted works.
- ❑ The Act requires that CMOs be accountable to both the copyright owners and the users of copyrighted works.
- ❑ CMOs are also required to be transparent about the distribution of royalties.

The Kenyan Copyright Act of 2001

- ❑ In 2019 one of the significant changes made to the Kenyan Copyright Act was the introduction of a penalty for online copyright infringement.
- ❑ The amendment made it an offense to upload or distribute copyrighted works over the internet without the permission of the copyright owner.
- ❑ The Act provides for compensation to the copyright owner, as well as damages to be paid by the infringing party.

594

- ❑ The **Copyright Act** generally gives the owner of copyright the exclusive right to do and authorise others to do the following:
 - ❑ Reproduce the work
 - ❑ Prepare derivative works based upon the work
 - ❑ Distribute copies of the work to the public by sale, lease, licensing or lending
 - ❑ Perform the work publicly
 - ❑ Display the copyrighted work publicly

595

- ❑ Copyrighted work may include the following:
 - ❑ Literary works such as computer software etc
 - ❑ Musical works including any accompanying words
 - ❑ Dramatic works including any accompanying music
 - ❑ Pantomimes and choreographic works
 - ❑ Pictorial graphics and sculptural works
 - ❑ Motion pictures and other audiovisual works
 - ❑ Sound recordings
 - ❑ Architectural works

CANNOT

596

- ❑ The following are not eligible for copyright protection:
 - ❑ Works consisting of entirely of information that is **common property** e.g.
 - ❑ standard calendars, height and weight charts, tape measures and rulers and lists of tables taken from public documents
 - ❑ Works that **have not been fixed in a tangible form of expression** e.g.
 - ❑ choreographic works that have not been recorded or improvised.
 - ❑ Speeches or performances that have not been written or recorded.

COPYRIGHT PROTECTION

Work that **CANNOT** Be ©

597

- ❑ Ideas, procedures, methods, systems, processes, concepts, principles, discoveries or devices.
 - ❑ The above should not copyrighted but patented
- ❑ Titles, names, short phrases and slogans, familiar symbols or designs, mere variations of typographic ornamentation, lettering or colouring
 - ❑ protect these with a trademark

COPYRIGHT PROTECTION

Criteria for ©

598

- ❑ For any work to qualify for copyright it must meet the following three criteria:
 - ❑ The work must be fixed in **tangible medium of expression**
 - ❑ It must be **original** created by the author and not copied from someone else
 - ❑ It must be **creative**

599

CLAIM FOR COPYRIGHT

- ❑ Copyright exists from the time the work is created in fixed form.
- ❑ In the case of **works made for hire** the employer and not the employee is considered to be the author.

CLAIM FOR COPYRIGHT

600

- ❑ Work for hire may include such things as:
 - ❑ A work prepared by an employee **within the scope of their employment**
 - ❑ Work **specially ordered or commissioned for use** such as:
 - ❑ A contribution to collective work
 - ❑ A part of motion picture or other audiovisual work
 - ❑ A translation
 - ❑ A supplementary work
 - ❑ A compilation
 - ❑ An instruction text
 - ❑ A test
 - ❑ Answer material for a test
 - ❑ An atlas

601

- ❑ The author (person who creates the work)
- ❑ The author's employer (if the author is employee)
 - ❑ Not necessary for there to be an IPR clause in the contract of employment
 - ❑ Copyright ownership will belong to the employer **UNLESS** a contract clause specifies otherwise
- ❑ Independent consultants own copyright unless the client insists on specifying otherwise in the contract

611

- ❑ **Fair dealing**
 - ❑ private study/research; criticism or review; reporting current events
 - ❑ It is **not** fair dealing to convert a low level program to a higher level language
- ❑ **Backup copies**
 - ❑ Max of one copy allowed.
 - ❑ None if supplied on non-volatile medium

612

- ❑ **Transfers of works**
 - ❑ If A sells copy to B, must retain no copies
- ❑ **Decompilation for the purpose of interoperability**
 - ❑ permitted if this is the only way to obtain information necessary to enable interoperability
 - ❑ Not permitted if owner publishes API

613

- ❑ **Error correction**
 - ❑ if necessary to its lawful use
 - ❑ provided this is not prohibited by any contract term
- ❑ **Databases**
 - ❑ a lawful user may download if necessary to access the contents or part of contents
 - ❑ Doing anything in relation to a database for commercial research is not fair dealing

615

- ❑ **Copying means reproducing the work in any material form.**
 - ❑ Covers loading into RAM, no matter how transient this is.
- ❑ Any use of digitised material requires the explicit consent of the copyright holder, a contrast with printed material and sound recordings, which can be read/heard freely.

616

- ❑ E.g. programmer changes jobs, then produces program of similar functionality to copyrighted one owned by former employer.
- ❑ US idea v expression tends to permit, but counts aspects of the logic as expression
- ❑ UK practice: what is copyright? Is it original? Did copying happen? Was it substantial?
- ❑ How about Kenya?

617

Can only be done with consent of copyright owner

Includes translating a work to a foreign language to a different computer language

Varieties of software licence: Commercial end user

623

- ❑ Single copy licence
 - ❑ restricted to one machine
 - ❑ sometimes eased to one machine at work and one at home or a portable
 - ❑ special terms for categories of user, e.g. student
- ❑ Multiple-copy licence
- ❑ Network licence
 - ❑ up to N images in simultaneous use
- ❑ Site/Department/Enterprise licence

624

- ❑ Developer's licence
- ❑ Shareware
- ❑ Free for non-commercial use
- ❑ Freeware
- ❑ GNU Public licence

625

- ❑ For programming language compilers, interpreters and environments
- ❑ Most modern languages rely on run-time interpreters or libraries, hence incorporate software owner's code in user-written code
- ❑ Right to distribute software may be free, restricted to those paying a higher licence fee, or require per-copy royalties

626

- ❑ Shareware is commercial software
 - ❑ freely distributed on a 'try before you buy' basis via archives
 - ❑ not free to use - sometimes referred to as 'honorware'
 - ❑ Professionals are obliged to respect such licences

627

- ❑ Commercially owned software made available for academic and individual users for **non-commercial purposes**
 - ❑ in hope of engendering brand loyalty among graduates, e.g. IBM, mSQL
- ❑ Free for R&D only
 - ❑ e.g. Oracle - Universities may use for research but not teaching or admin, which are revenue-earning activities

628

- ❑ Still proprietary
 - ❑ Users and developers pay no fee
 - ❑ May have restricted rights to develop, incorporate in products, access source
 - ❑ Must indemnify owner from all claims
 - ❑ Must preserve all copyright notices and licence terms
 - ❑ Problem for commercial vendors who must support own products

629

- ❑ Dedicated to FSF principle that software can be freely accessed and distributed
 - ❑ i.e. not necessarily free as in no £/\$/Ksh
 - ❑ Sometimes you are asked for donations
 - ❑ Some producers and distributors make money from providing support
- ❑ Source code must be distributed with package or freely obtainable from net
- ❑ Redistributors and value-added resellers must pass on all notices and source code and make the whole product GPL

631

❑ **Literary works**

- ❑ The protection is available to **published** or **unpublished** works.
- ❑ Both **source code** and **object code** are taken to be literary works.
- ❑ Hence they are copyrightable.

632

- ❑ Copyright protects creators of intellectual property from having their work copied by others for any purpose.
- ❑ In Kenya, the duration is the life of the author plus an additional 50 years after the author's death.
- ❑ The intent behind copyright laws is to encourage creativity and authorship.
- ❑ Creative people receive financial and other benefits of their work.

633

- ❑ Many countries/nations have their own copyright laws.
- ❑ They also ratify international conventions and bilateral agreements on IPR.
- ❑ Copyright laws allows the buyer to use the software while the creator retains legal title.
- ❑ Copyright protects against copying of parts of or the entire programs.
- ❑ Damages and relief are awarded for infringement.

634

❑ Disadvantage:

- ❑ The underlying **ideas** behind a work are not protected, only their **manifestation** in a work.
- ❑ A competitor can use your software, understand how it works, and build new software that follows the same concepts without infringing on a copyright...

635

- ❑ “**Look and feel**” copyright infringement lawsuits are about differentiating between an idea and its expression.
- ❑ E.g. in the early 1990s **Apple Computer sued Microsoft Corporation and Hewlett-Packard** for infringement of the expression of Apple’s Macintosh interface.
- ❑ They claimed that the defendants copied the **expression** of overlapping windows.

636

- ❑ The defendants countered that the **idea** of overlapping windows can be **expressed** only in a single way ...
- ❑ Thus it was not protectable under the **merger doctrine** of copyright law:
 - ❑ When **ideas and their expression merge**, the expression cannot be copyrighted.
- ❑ In general, courts appear to be following the reasoning of the **Brown Bag Software vs. Symantec Corp (1989)** case.
 - ❑ The court found that similar concept, function, general functional features (e.g., drop-down menus), and colors are not protectable by copyright law.

637

COPYRIGHT PROTECTION

- ❑ Copyright is ...
- ❑ a form of ownership ...
- ❑ that excludes others,
- ❑ for a limited amount of time,
- ❑ from copying without permission.

COPYRIGHT PROTECTION

638

- ❑ You can NOT copyright an idea.
- ❑ Q: What, then, can you copyright?
- ❑ The **expression of an idea**.
- ❑ What is the difference?
- ❑ One way to look at it:
 - ❑ The idea is the **concept**, the expression is the **way it is realised**.
 - ❑ The expression would be the exact words in the work.

639

COPYRIGHT PROTECTION

- ❑ What is protected is the **fixation of an idea in a tangible medium of expression**,
- ❑ We can’t protect the idea itself, or any processes or principles associated with it.
- ❑ The distinction is not always clear and is usually on a case by case basis.
- ❑ **Source and object codes** are copyrightable because they are **expressions of ideas**.

COPYRIGHT PROTECTION

640

- ❑ A problem arises here.
- ❑ It is very, very simple to make a whole new app by changing very little in an existing software.
- ❑ Think back to the case study of the fantastic software start-up that collapsed due to piracy.
- ❑ To what does the copyright apply?
 - ❑ The old version?
 - ❑ The parts of the new version with the old code?

COPYRIGHT PROTECTION

641

- ❑ In this case, this question arises even when you, the owner modifies the app.
- ❑ Should you reapply for copyright each time you add new pieces of code?
- ❑ Maybe viewing software as 'literary works' is over simplifying the issue ...

Is Software Literature?

642

Literature

- ❑ Doesn't change much.
- ❑ If I create a literary work similar to yours I can acquire protection for it if I did it independently and it is **literally different**.
- ❑ For literature to be useful, a user must be present

Software

- ❑ Constantly changing.
- ❑ If I independently develop software strikingly similar to yours, I may not be able to copyright it (cf: *Whelan vs Jaslow*)
- ❑ Software behaviour is useful in itself, even with no users.

Case Law

643

- ❑ **Franklin Computer Corp versus Apple (1984)**
- ❑ Apple had proprietary software that could only run on the Apple II.
- ❑ Franklin developed a clone, the Franklin ACE 1000 whose ROM and OS were indisputably copied from Apple (practically line by line).
 - ❑ The programs were in object code stored in ROM.
- ❑ He was found guilty of copyright infringement.

Case Law

644

- ❑ An appeals court held that:
 1. a computer program, whether in **object code** or **source code**, is a "**literary work**" and is protected from unauthorised copying
 2. a computer program in object code embedded in ROM chip is an appropriate subject of copyright;
 - *Franklin had argued that*
 - (1) Apple's software existed only in machine-readable form (not in printed form), and
 - (2) some of the software did not contain copyright notices.

Case Law

645

3. computer operating system programs are not per se precluded from copyright protection;
 - ❑ (first time a court had ruled that an OS was copyrightable)
4. even without a presumption of irreparable harm generally applied in copyright infringement actions, the jeopardy to the copyright holder's investment and competitive position caused by a competitor's wholesale copying of many of the copyright holder's key operating programs would satisfy the requirement of irreparable harm needed to support a preliminary injunction.
5. Irreparable harm must be presumed in every copyright case.
 - ❑ (A lower court had found that Franklin's was too small a company to pose any serious threat to Apple but granting Apple a preliminary injunction would probably bankrupt Franklin.

Case Law

646

- ❑ **Whelan versus Jaslow (1987):**
- ❑ Whelan developed a program for Jaslow in Fortran.
- ❑ The agreement was that Whelan would own it.
- ❑ Jaslow then redid the program line by line in BASIC.
- ❑ Whelan sued.

Case Law

647

- ❑ Though Jaslow's program was *literally different* and maybe even a different expression of the same idea, the court found in favour of Whelan.
- ❑ They found *comprehensive non-literal similarity*.
 - ❑ It may not be a literal copy (of the text of the code), but the (more abstract) **structure, sequence and organisation** (SSO) were copied.
- ❑ **cf Lotus vs Borland (1996) Idea vs expression of an idea**

648

- ❑ Digital representation of IP has made it easier to infringe copyright, and policing of copyright infringement has become difficult.
 - ❑ The Internet is one area where this has become very difficult due to the number of people who are performing copying of IP.
- ❑ One point of contention is **fair use** of copyrighted material that are copied for personal use, education or research and not for commercial purpose.

649

- ❑ Copying may be allowed in the licence e.g. for fair use and back-up purposes.
- ❑ **Fair use:**
- ❑ Teaching
- ❑ Scholarly work/research
- ❑ Criticisms or comments
- ❑ News reporting
- ❑ Some governmental purposes e.g.:
 - ❑ parliamentary/judiciary proceedings
 - ❑ commissions and statutory inquiries.

650

- ❑ Computer Software is considered as copyrightable material including freeware, shareware, and commercial software.
- ❑ Only **public domain** and **open source software** fall outside the copyrighted restrictions.
- ❑ When you buy software you are bound by the license agreement.
- ❑ License agreements allow you to **use** the software and **not to modify, sell or give it away** as those rights belong to the copyright holder.

651

- ❑ Digital images like photographs, art-like cartoons or complex images are copyrighted material
 - ❑ but under **fair use** a downloaded image can be used as a screen saver
 - ❑ but you are not allowed to distribute or post it in your own web site.
- ❑ **Plagiarism**
 - ❑ under the fair use practices you can include someone's work **as long as you identify the source**.

652

The Kenyan Copyright Act

The Kenyan Copyright Act of 2001

- Kenya has a robust intellectual property rights (IPR) legal framework.
- This framework primarily falls under copyright law, which is aimed at protecting the creativity of individuals, authors, and artists.
- The Kenyan Copyright Act of 2001 governs copyright law in the country.
- It takes a comprehensive approach to the protection of literary, artistic, musical, and other creative works.
- It outlines:
 - the rights of copyright owners
 - limitations on exclusive rights
 - remedies available to parties in cases of infringement.

The Kenyan Copyright Act of 2001 The Rights of Copyright Owners

- Protects original works of art, including music, broadcasts, films, photographs, and literary works.
- Gives exclusive rights to copyright owners to:
 - reproduce, distribute, display, and perform their work.
 - create a derivative work or adaptation of their work.

The Kenyan Copyright Act of 2001 Limitations On Exclusive Rights

- The Act defines the limitations on these exclusive rights e.g.:
 - the use of work for educational, scientific, and research purposes may be allowed in certain circumstances.
- However, such use must not infringe on the rights of the copyright owner.

The Kenyan Copyright Act of 2001 Remedies

- The Act outlines the remedies available to parties who are affected by copyright infringement.
- These remedies include civil and criminal action.
- In civil proceedings, a copyright owner can seek an injunction to stop an infringing party from continuing an action that infringes on their rights.
- They can also claim damages and seek an account of profits made by the infringing party.
- In criminal proceedings, an infringing party can face imprisonment and fines.

The Kenyan Copyright Act of 2001

- The Kenyan Copyright Act also outlines the role of collective management organisations (CMOs).
- These are registered under the Act and are responsible for **administering the licenses** for the use of copyrighted works.
- The Act requires that CMOs be accountable to both the copyright owners and the users of copyrighted works.
- CMOs are also required to be transparent about the distribution of royalties.

The Kenyan Copyright Act of 2001

- ❑ In 2019 one of the significant changes made to the Kenyan Copyright Act was the introduction of a penalty for online copyright infringement.
- ❑ The amendment made it an offense to upload or distribute copyrighted works over the internet without the permission of the copyright owner.
- ❑ The Act provides for compensation to the copyright owner, as well as damages to be paid by the infringing party.

- ❑ The **Copyright Act** generally gives the owner of copyright the exclusive right to do and authorise others to do the following:
 - ❑ Reproduce the work
 - ❑ Prepare derivative works based upon the work
 - ❑ Distribute copies of the work to the public by sale, lease, licensing or lending
 - ❑ Perform the work publicly
 - ❑ Display the copyrighted work publicly

- ❑ Copyrighted work may include the following:
 - ❑ Literary works such as computer software etc
 - ❑ Musical works including any accompanying words
 - ❑ Dramatic works including any accompanying music
 - ❑ Pantomimes and choreographic works
 - ❑ Pictorial graphics and sculptural works
 - ❑ Motion pictures and other audiovisual works
 - ❑ Sound recordings
 - ❑ Architectural works

CANNOT

- ❑ The following are not eligible for copyright protection:
 - ❑ Works consisting of entirely of information that is **common property** e.g.
 - ❑ standard calendars, height and weight charts, tape measures and rulers and lists of tables taken from public documents
 - ❑ Works that **have not been fixed in a tangible form of expression** e.g.
 - ❑ choreographic works that have not been recorded or improvised.
 - ❑ Speeches or performances that have not been written or recorded.

COPYRIGHT PROTECTION Work that **CANNOT** Be ©

- ❑ Ideas, procedures, methods, systems, processes, concepts, principles, discoveries or devices.
 - ❑ The above should not be copyrighted but patented
- ❑ Titles, names, short phrases and slogans, familiar symbols or designs, mere variations of typographic ornamentation, lettering or colouring
 - ❑ protect these with a trademark

COPYRIGHT PROTECTION Criteria for ©

- ❑ For any work to qualify for copyright it must meet the following three criteria:
 - ❑ The work must be fixed in **tangible medium of expression**
 - ❑ It must be **original** created by the author and not copied from someone else
 - ❑ It must be **creative**

CLAIM FOR COPYRIGHT

664

- Copyright exists from the time the work is created in fixed form.
- In the case of **works made for hire** the employer and not the employee is considered to be the author.

CLAIM FOR COPYRIGHT

665

- Work for hire may include such things as:
 - A work prepared by an employee **within the scope of their employment**
 - Work **specially ordered or commissioned for use** such as:
 - A contribution to collective work
 - A part of motion picture or other audiovisual work
 - A translation
 - A supplementary work
 - A compilation
 - An instruction text
 - A test
 - Answer material for a test
 - An atlas

666

- The author (person who creates the work)
- The author's employer (if the author is employee)
 - Not necessary for there to be an IPR clause in the contract of employment
 - Copyright ownership will belong to the employer **UNLESS** a contract clause specifies otherwise
- Independent consultants own copyright unless the client insists on specifying otherwise in the contract

676

- **Fair dealing**
 - private study/research; criticism or review; reporting current events
 - It is **not** fair dealing to convert a low level program to a higher level language
- **Backup copies**
 - Max of one copy allowed.
 - None if supplied on non-volatile medium

677

- **Transfers of works**
 - If A sells copy to B, must retain no copies
- **Decompilation for the purpose of interoperability**
 - permitted if this is the only way to obtain information necessary to enable interoperability
 - Not permitted if owner publishes API

678

- **Error correction**
 - if necessary to its lawful use
 - provided this is not prohibited by any contract term
- **Databases**
 - a lawful user may download if necessary to access the contents or part of contents
 - Doing anything in relation to a database for commercial research is not fair dealing

680

- ❑ Copying means reproducing the work in any material form.
 - ❑ Covers loading into RAM, no matter how transient this is.
- ❑ Any use of digitised material requires the explicit consent of the copyright holder, a contrast with printed material and sound recordings, which can be read/heard freely.

681

- ❑ E.g. programmer changes jobs, then produces program of similar functionality to copyrighted one owned by former employer.
 - ❑ US idea v expression tends to permit, but counts aspects of the logic as expression
 - ❑ UK practice: what is copyright? Is it original? Did copying happen? Was it substantial?
 - ❑ How about Kenya?

682

Can only be done with consent of copyright owner

Includes translating a work to a foreign language to a different computer language

Varieties of software licence: Commercial end user

688

- ❑ Single copy licence
 - ❑ restricted to one machine
 - ❑ sometimes eased to one machine at work and one at home or a portable
 - ❑ special terms for categories of user, e.g. student
- ❑ Multiple-copy licence
- ❑ Network licence
 - ❑ up to N images in simultaneous use
- ❑ Site/Department/Enterprise licence

689

- ❑ Developer's licence
- ❑ Shareware
- ❑ Free for non-commercial use
- ❑ Freeware
- ❑ GNU Public licence

690

- ❑ For programming language compilers, interpreters and environments
- ❑ Most modern languages rely on run-time interpreters or libraries, hence incorporate software owner's code in user-written code
- ❑ Right to distribute software may be free, restricted to those paying a higher licence fee, or require per-copy royalties

- 691
- ❑ Shareware is commercial software
 - ❑ freely distributed on a 'try before you buy' basis via archives
 - ❑ not free to use - sometimes referred to as 'honorware'
 - ❑ Professionals are obliged to respect such licences

- 692
- ❑ Commercially owned software made available for academic and individual users for **non-commercial purposes**
 - ❑ in hope of engendering brand loyalty among graduates, e.g. IBM, mSQL
 - ❑ Free for R&D only
 - ❑ e.g. Oracle - Universities may use for research but not teaching or admin, which are revenue-earning activities

- 693
- ❑ Still proprietary
 - ❑ Users and developers pay no fee
 - ❑ May have restricted rights to develop, incorporate in products, access source
 - ❑ Must indemnify owner from all claims
 - ❑ Must preserve all copyright notices and licence terms
 - ❑ Problem for commercial vendors who must support own products

- 694
- ❑ Dedicated to FSF principle that software can be freely accessed and distributed
 - ❑ i.e. not necessarily free as in no £/\$/Ksh
 - ❑ Sometimes you are asked for donations
 - ❑ Some producers and distributors make money from providing support
 - ❑ Source code must be distributed with package or freely obtainable from net
 - ❑ Redistributors and value-added resellers must pass on all notices and source code and make the whole product GPL

718 The Case for Software as IP

- 719
- ❑ The eligibility of computer software for these forms of protection is contentious.
 - ❑ It is still being decided by courts and legislatures

720

- With software, what can be owned?
 - The algorithm?
 - The source code?
 - The object code?
 - The user interface?
 - The copy on disk?
 - The right to use?

721

- With software, what can be owned?
- The algorithm?
 - *abstract method of solution ...*
 - *the sequence of machine commands that the source code and object code represent.*

722

- The source code?
 - *step by step solution to a problem,*
 - *written by the programmer(s)*
 - *using one or more **algorithms***
 - *usually in a high-level computer language*

723

- The object code?
 - *a machine-language translation of the source code*
 - *It actuates the setting of switches to enable the computer to perform the underlying algorithm*

724

- The user interface?
 - *The "look and feel" of a program, i.e. how the program appears on the screen and interfaces with users.*

725

- The copy on disk?
- The right to use?

Is Software IP?

726

- ❑ Software challenges traditional notions about property and ownership.
- ❑ In the 1970s, it was difficult to patent software due to the sw being perceived as:
 - ❑ a mental process
 - ❑ a mathematical algorithm

Is Software IP?

727

- ❑ ***Diamond versus Diehr (1981)***
- ❑ The plaintiff (Diehr) had applied for a **patent** on a process for curing synthetic rubber.
- ❑ His machine could cure rubber with the help of a computer using mathematical formulae.

Is Software IP?

728

- ❑ The defendant, Diamond, the **patent examiner**, rejected his application.
- ❑ This was on the basis that the steps were carried out by a computer under the control of a stored program.
- ❑ The question here was *whether patentable claims become invalid because they include mathematical formulas.*
- ❑ **Held:** Patentable claims do not become invalid because they include mathematical formulas.

Is Software IP?

729

- ❑ After this case, many patents have been granted on software.
- ❑ A new combination of steps in a process may be patentable ...
- ❑ even though all the parts of the combination were well known and commonly used before the combination was made.
- ❑ One of Diehr (the patent applicant)'s arguments;
- ❑ *Yes, a mathematical formula, just like a law of nature, cannot be the subject of a patent ...*

Is Software IP?

730

- ❑ However they were seeking protection for a **process** of curing synthetic rubber, not a mathematical formula.
- ❑ Sure, their process used a well-known mathematical equation.
- ❑ However they were not stopping anyone from using it unless ...
- ❑ it was in conjunction with all of the other steps in their claimed process.

Arguments against Software Protection

Arguments against Software Protection

732

- A person that owns a program owns the mental steps that make up the program.
- Thus you cannot use these mental steps.
- That is basically interfering with your freedom of thoughts.
 - Imagine someone claiming ownership of the IF statement.
- The level of knowledge considered is generic and common.

Arguments against Software Protection

733

- But what about those who argue that:
"No ownership → lack of incentive to produce software."
- Says who?
- Not all programmers do it for the money.

Arguments against Software Protection

- Information wants to be free.
- Information wants to be shared.

Arguments against Software Protection

- **Information wants to be free:**
- Richard Stallman = strong proponent.
- He opposes software IPR:
 - Programmers would still write programs even without financial rewards via copyright protections.

Arguments against Software Protection

- According to Stallman:
 - Information is something that we humans desire to share with one another.
 - Software development is like science.
 - It progresses most rapidly when knowledge is shared openly.

Arguments against Software Protection

- To share information, it must be communicated.
- Intricate IP structures and mechanisms prohibiting / discouraging the communication of information undermine its very purpose – as something to be shared.

Arguments against Software Protection

- ❑ **Information wants to be shared.**
- ❑ Herman Tavani is a proponent.
- ❑ He argues that **Information Wants to be Shared** has a better chance at being taken seriously than **Information Wants to be Free**.

Arguments against Software Protection

- ❑ Sir Tim Berners-Lee, invented HTTP, and the WWW.
- ❑ He shared it freely with the world.
- ❑ The idea behind HTTP was to allow for the sharing of information.
- ❑ Doug Englebart freely shared his invention with everybody.
- ❑ He did not claim a patent for the mouse.

Arguments against Software Protection

- ❑ Such information sharing has benefited many entrepreneurs.
- ❑ Some of them then sought to control the flow of information in cyberspace.
 - ❑ Steve Jobs got his ideas of GUIs from Xerox PARC.
 - ❑ MS Windows's UI was derived from his ideas.
 - ❑ Current UIs have benefited from the sharing of information.

Arguments against Software Protection

- ❑ The Open Source movement supports the idea that **Information Wants To Be Shared**.
- ❑ We need to preserve the intellectual commons.
- ❑ **Q:** What if all the information that we have traditionally shared freely were to disappear from the public domain and enter the world of copyright protection?

Arguments against Software Protection

- ❑ **Short term effect:**
 - ❑ Private corporations and some individuals will make huge profits.
- ❑ **Long term effect:**
 - ❑ Society may be worse off intellectually, spiritually, and even economically.
- ❑ The short-term goals or privatisation of information should be balanced against the interests of the greater public.

Further Reading

- ❑ John Locke, *Two Treatises of Government* (P. Laslett, ed., Cambridge: Cambridge University Press, 1970), Second Treatise, Sec. 27. 4
- ❑ Bentham, Jeremy (January 2009). *An Introduction to the Principles of Morals and Legislation* (Dover Philosophical Classics). Dover Publications Inc. p. 1. ISBN 978-0486454528.
- ❑ Also:
 - ❑ For a not recent but still thought provoking and informative discussion on the Kenyan scene with regards to IP (including procedures to follow when applying for the protections), read <http://viffaconsult.co.ke/intellectual-property-a-case-review-of-kenyas-it-sector/>

Why Should We Care About Legal and Professional Issues?

744

- We've already established that
 1. Today, technology plays a huge role in our society.
 2. We must take into consideration its ethical, social and legal implications.

Why Should We Care About Legal and Professional Issues?

745

- What are the repercussions of the technology we apply?

Exponential growth in computer usage
+
increase in monetary value of software and computer related technologies
=
software professionals being increasingly affected by the legal issues surrounding these technologies

Why Be Concerned About Ethics and Professional Conduct?

746

- Certain legal frameworks apply to our discipline and the areas in which we work.
- As computing professionals, we must work within them. E.g.:
 - ▣ It is now essential for software professionals to understand intellectual property categories.
 - ▣ We must understand how they specifically relate to software and computer related developments:
 - trade secrets,
 - trademarks,
 - and especially copyrights and patents

Why Be Concerned About Ethics and Professional Conduct?

747

- We are also bound to the ethical and moral principles appropriate to computing operations.
- Legal, professional and ethical issues are ALL important in computing.

CAT (30 MARKS)

Groupwork: Paper

INSTRUCTIONS

- Divide yourselves into not more than 10 groups.
- In a SPREADSHEET app type your member details into 4 columns as follows:

S/NO	Truncated Reg No	Reg No	Name
1	12345/2020	A12/12345/2020	MARY ALI
2			
3			
...			
...			

Name the spreadsheet **SCO402L&E 2024-2025 Sem1 Group Members**

CAT (30 MARKS)

- Provide a comprehensive overview of the process for acquiring intellectual property rights (IPR) on computing property, such as software or algorithms, in Kenya.
- In your paper, include the legal steps, required documentation, and key considerations from the initial creation of a computing product to the final grant of IPR protection in the context of Kenyan intellectual property law.

CAT (30 MARKS)

☛ Summary of documents you will send to my email:

1. A spreadsheet named:
SCO402L&E 2024-2025 Sem1 Group Members
2. A word processed (NOT a pdf) document named:
SCO402L&E 2024-2025 Sem1 CAT2

☛ **NOTE**

1. Send these documents to my email address on or before Friday, 17th November, 2023.
2. The subject of the email MUST be SCO402L&E 2024-2025 Sem1 CAT2
3. Plagiarism will not be tolerated.

AI

The Ethical Implications

Ethical Dilemmas and AI

- Ethical dilemmas in AI and machine learning are multifaceted.
- They span issues including:
 - the intersection of emerging technologies
 - bias
 - accountability
 - employment
 - health

Emerging Technologies and Ethical Dilemmas

- This addresses ethical challenges arising from emerging technologies like
 - AI
 - Biotechnology
 - The convergence of AI and biotechnology
 - e.g., genetic editing and personalised medicine)
 - neurotechnology.

Emerging Technologies and Ethical Dilemmas

- They raise new ethical questions:
 - AI is great but
 - risks like bots spreading misinformation, automated hacking, lethal autonomous weapons.
 - Biotechnology advancements in gene editing, prosthetics or implants can enhance humans - but
 - blurred lines between health and enhancement.
 - Neurotechnology like reading brain signals has medical benefits but
 - privacy concerns if data is misused.

Emerging Technologies and Ethical Dilemmas

- ❑ The US's CRISPR is a gene editing technology that allows DNA to be edited with precision and relative ease.
- ❑ It has promising medical applications like curing genetic diseases
 - ❑ there are clinical trials using CRISPR for e.g., sickle cell anemia, cancer, blindness.

Emerging Technologies and Ethical Dilemmas

- ❑ However. It also raises bioethical and legal uncertainties:
 - ❑ Editing embryo DNA is controversial and currently illegal for use in human reproduction in the US.
 - ❑ But. In 2018 a Chinese scientist claimed he edited embryos to create the first CRISPR babies, raising global alarm.
 - ❑ Germline editing: changes can be passed on to future generations.

Emerging Technologies and Ethical Dilemmas

- ❑ Pose complex challenges for ethicists:
 - ❑ Weigh benefits against potential harms from misuse of technology.
 - ❑ Update policies and regulations to keep pace with rapid technological change.
 - ❑ e.g., for gene editing, regulations should be updated to keep pace with the technology, balance risks and benefits, and restrict use that could affect *heritable* traits.
 - ❑ Involve diverse perspectives (public, private, academia) in governance.
 - ❑ Ensure human rights are protected as technologies evolve.

AI Bias

- ❑ Bias in AI refers to the presence of **systematic** and **unfair** preferences for certain groups over others.
 - ❑ Fairness involves ensuring that AI algorithms treat all individuals or groups equitably.
 - ❑ **Systematic preferences**
 - ❑ consistent and patterned favouritism or bias toward certain groups or individuals *within a system or process*.
 - ❑ Visible in AI and machine learning when algorithms **consistently** exhibit a tendency to favour specific characteristics, attributes, or demographics over others.

Bias and Fairness in AI Algorithms

- ❑ Algorithmic bias can lead to discrimination and unfair outcomes:
 - ❑ Health insurer UnitedHealth Group used an algorithm to help health providers determine which patients should receive extra medical care and support.
 - ❑ However. Analysis found the algorithm was biased:
 - ❑ a study published in the journal *Science* in October 2019 revealed the algorithm was favouring white patients over **sicker** black patients for healthcare programs.

Bias and Fairness in AI Algorithms

- ❑ January 2020 - UnitedHealth Group announced they would suspend use of the algorithm following the research findings.
- ❑ March 2020 - Congress opened an investigation into the algorithmic bias.
- ❑ April 2020 - UnitedHealth Group representatives testified to Congress that the algorithm was flawed and they regretted implementing it without more thorough bias testing.

Bias and Fairness in AI Algorithms

- ❑ Algorithmic bias can lead to discrimination and unfair outcomes:
 - ❑ The COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) is a proprietary algorithm used in the US criminal justice system.
 - ❑ It is a risk assessment tool designed to aid judges in predicting the likelihood of a defendant committing future crimes/re-offending.
 - ❑ It evaluates various factors related to an individual's criminal history and personal characteristics to generate a risk score.
 - ❑ It is used by judges for bail and sentencing decisions in many US states.
- ❑ Investigative analysis in 2016 found the COMPAS model was biased against black defendants.
 - ❑ they were more often incorrectly flagged as high risk compared to white defendants.

Bias and Fairness in AI Algorithms

- ❑ Other examples:
 - ❑ In 2020, the UK's Office of Qualifications and Examinations Regulation (Ofqual) implemented an algorithm to calculate grades for students after exams were canceled due to the COVID-19 pandemic.
 - ❑ The algorithm was supposed to standardise grades based on schools' historical performance.
 - ❑ However, students from schools with historically lower performance were disproportionately downgraded.
 - ❑ i.e., a bias against students from poorer backgrounds.
 - ❑ After widespread criticism, the UK government decided to abandon the algorithm and instead use teachers' predicted grades.

Bias and Fairness in AI Algorithms

- ❑ The use of AI in recruitment platforms raises concerns about gender and racial biases.
- ❑ In China, facial recognition algorithms have higher error rates for ethnic minorities like Uyghurs.
- ❑ The application of AI in credit scoring systems raises concerns about economic bias ...

Bias and Fairness in AI Algorithms

- ❑ E.g., in Kenya, access to financial services and credit is a major challenge due to lack of credit histories.
- ❑ AI and machine learning models are being adopted by banks and lenders to evaluate creditworthiness using alternative data.
 - ❑ e.g. the EazzyLoan using AI to analyse mobile phone data, financial transactions, social media to generate credit scores.
- ❑ Advocates argue AI increases access to credit by evaluating diverse indicators beyond traditional metrics like employment history.

Bias and Fairness in AI Algorithms

- ❑ However. Concerns around data privacy, fairness, and transparency of the AI models.
 - ❑ e.g. such an AI lending model may favour applicants with stronger digital footprints, potentially disadvantaging poorer populations.
- ❑ Oversight is limited as Kenya currently lacks comprehensive regulations governing use of AI systems.
- ❑ These example cases demonstrate how racial bias can be perpetuated through AI algorithms if discrimination and fairness are not addressed in the **development process**.

How To Increase Fairness

- ❑ Ensure diverse data sets for training algorithms.
- ❑ Continuously test for bias during development.
- ❑ Use technical bias audit tools to check for potential biases in your systems
 - ❑ problem is most are developed in the US
 - ❑ they may not tally with our laws and regulations
- ❑ Enable human oversight and auditing.
- ❑ Increase transparency in algorithms and use explainable AI.

AI Decision-Making and Accountability

- ❑ AI decision-making involves the process by which AI systems make choices or recommendations.
- ❑ As we've already seen, AI systems are increasingly used in high impact decisions like loan approvals, healthcare, and criminal justice.
- ❑ However, they lack human judgement to consider special circumstances.
- ❑ Accountability pertains to assigning responsibility for the outcomes of AI decisions.
 - ❑ It is challenged when adverse outcomes occur.

AI Decision-Making and Accountability

- ❑ US's Compas (the AI used to predict future criminals, with questionable accuracy and oversight).
- ❑ Tesla's autopilot, the advanced driver assistance system available on Tesla vehicles since 2014.
 - ❑ It uses cameras, sensors and AI to automatically control features like steering, accelerating, braking, and lane changes under certain conditions.
 - ❑ Questions have been raised about its accountability, reliability and the potential for misuse (it may give drivers a false sense of security, leading to lapses in attention).

AI Decision-Making and Accountability

- ❑ Tesla claims the system requires driver oversight and does not make the car autonomous.
- ❑ However, there have been fatal accidents where drivers overly relied on autopilot leading to collisions.
- ❑ Consumer groups have raised concerns about
 - ❑ safety
 - ❑ requiring too much driver attention
 - ❑ potential overstatement of its capabilities by Tesla.
- ❑ Thus the ethical implications involve questions about the appropriate level of autonomy, user responsibility, and the need for clear communication (by Tesla) about system limitations to ensure safe usage.

AI Decision-Making and Accountability

- ❑ In the UK, authorities use AI to sort through social security benefits claims and assess eligibility.
 - ❑ Their Department of Work and Pensions (DWP) use AI to identify patterns in claims that could indicate error or fraud.
 - ❑ Applicants struggle to appeal automated rejections.
- ❑ Use of AI in legal systems prompts discussions on accountability for algorithmic decisions.
- ❑ In China, AI is used to track and profile citizens to assess their trustworthiness.
 - ❑ Social credit systems utilising AI raised concerns about accountability and transparency.
 - ❑ Critics argue it can be used to limit dissent.
- ❑ Loan approval algorithms and AI-driven healthcare diagnosis systems also prompt discussions on accountability.

AI Decision-Making and Accountability

- ❑ Ways forward:
 - ❑ Humans must remain ultimately accountable for impactful AI systems.
 - ❑ Transparency, oversight and appeal mechanisms must exist.
 - ❑ Red lines must be drawn on use of AI that can infringe on human rights.

AI and Employment

- ❑ AI has impacted employment
 - ❑ e.g. job displacement, job creation, and changes in the nature of work.
- ❑ AI is automating certain tasks and displacing some jobs.
 - ❑ Low skilled jobs are most at risk.
 - ❑ e.g. in sectors like manufacturing, ecommerce and transport
 - ❑ productivity improves but job creation is moderated
- ❑ Adoption of AI in agriculture affects traditional farming practices and jobs.
- ❑ Administrative roles also threatened.
 - ❑ E.g., chatbots and automation in customer service impact employment in call centers.

AI and Employment

- But. AI also creates new kinds of jobs.
 - New kinds of AI and skilled tech jobs are increasing.
 - Increased demand for specialists to develop and manage AI systems.
- Also, roles that require human skills like creativity, empathy and judgement are harder to automate.
- Businesses and governments must invest in re-training programmes and support displaced workers.
- Educational reforms should focus on adaptability.
- Labor policies should evolve to protect workers and support lifelong learning in the AI age.

AI in Healthcare

- AI systems are increasingly used in healthcare e.g., for
 - administrative functions
 - medical medical imaging analysis and diagnostics.
 - Machine learning can automate analysis of images from x-rays, MRIs, CT scans to detect abnormalities and diseases.
 - The U.S. Food and Drug Administration (FDA) has approved several AI imaging tools like those detecting strokes, fractures, brain aneurysms.
 - treatment recommendations
 - drug development

AI in Healthcare

- Benefits of AI in healthcare:
 - huge volumes of patient and medical data can be easily analysed to discover new insights.
 - faster and earlier diagnosis
 - more accessible expertise
 - more personalised and precision medicine is possible.
 - human errors and overhead costs can be reduced.
 - access to healthcare in under-served communities can be expanded.

AI in Healthcare

- However. Ethical concerns when treatment decisions rely on AI analysis include:
 - Patient privacy and data security risks when medical data is used for system training.
 - Transparency and accountability for wrong diagnoses or treatment recommendations.
 - patient informed consent
 - Displacement of medical personnel
 - Degradation of medic skills due to over-reliance on AI .
 - Amplification of existing healthcare biases and inequalities (due to bias in training data)
 - Safe and effective integration of AI with clinical workflows.

AI in Healthcare

- Adoption of AI in medical diagnostics is increasing.
- However, physician oversight is still needed.
- Also, ethical frameworks to ensure patient confidentiality and consent are required.

AI in Healthcare

- Ways to address ethical risks:
 - Strict data governance policies and consent mechanisms for training data.
 - Oversight and auditing of AI systems to validate recommendations.
 - Keep physicians involved in decisions to combine AI and human expertise.
 - Monitor AI systems for signs of bias and adjust algorithms accordingly.

Trends in Technology Ethics and Legal Frameworks

- ❑ Public debate on technology's impact must continue.
- ❑ Technology ethics must continually evolve.
- ❑ Legal frameworks to regulate AI and emerging technologies must be developed.
- ❑ We must
 - ❑ update policies wisely
 - ❑ invest in people-centric science
 - ❑ ensure ethics keeps pace with innovation.

Trends in Technology Ethics and Legal Frameworks

- ❑ Looking ahead, necessary trends in governing emerging technologies include:
 - ❑ International and national **AI safety and ethics guidelines** to align responsible development.
 - ❑ Industries forming **ethics boards and standards bodies** to self-regulate.
 - ❑ Governments updating **privacy and consumer protection laws** related to AI.

Trends in Technology Ethics and Legal Frameworks

- ❑ Rights-based **global agreements** to govern use of technologies like autonomous weapons.
- ❑ More **public-private partnerships** to fund and regulate new technologies.
- ❑ More emphasis on **ethics education and training** for technologists and policy-makers.

Trends in Technology Ethics and Legal Frameworks

- ❑ US: Ongoing discussions on federal AI regulations and ethical guidelines.
- ❑ UK: Development of ethical AI frameworks by organisations like the Centre for Data Ethics and Innovation.
- ❑ In Oct 2023 the UK government announced through a press release that companies can apply for up to £400,000 in government investment to fund innovative new solutions which tackle bias and discrimination in AI systems.
- ❑ China: Integration of AI ethics in the country's Five-Year Plans.
 - ❑ China's 2021 14th Five-Year Plan and Vision 2030 both place a strong focus on the development of the digital economy.

Trends in Technology Ethics and Legal Frameworks

- ❑ Kenya: Consideration of data protection laws to address ethical concerns in technology.
 - ❑ we need stronger/more focused data protection laws to address ethical concerns in technology.
- ❑ The Kenya DPA, 2019 has some progressive provisions in relation to automated decisions.
- ❑ However,
 - ❑ compliance and enforcement have been weak.
 - ❑ it only applies to personal data.
 - ❑ Non personal data can be used as training data - and train the AI to be discriminatory.
- ❑ A better approach may be the enactment of a comprehensive non-discrimination statute that addresses the unique challenges of algorithmic bias.

References

1. Bembenek, E., Nissan, R., & Obermeyer, Z. (2021, October 21). To stop algorithmic bias, we first have to define it. Brookings.
2. Department for Science, Innovation and Technology, Centre for Data Ethics and Innovation, Information Commissioner's Office, Equality and Human Rights Commission, & Viscount Camrose. (2023, October 16). New innovation challenge launched to tackle bias in AI systems. GOV.UK. Retrieved October 18, 2023, from <https://www.gov.uk/government/news/new-innovation-challenge-launched-to-tackle-bias-in-ai-systems>
3. Donovan, K. P., & Park, E. (2021, November). Algorithmic Intimacy: Curious Utopias [Preprint]. Social Anthropology.
4. Doudna, J. (2017, Nov 5). Jennifer Doudna: CRISPR Basics [Video]. YouTube. <https://www.youtube.com/watch?v=47pkFey3CZ0>
5. nature video. (2017, Oct 31). CRISPR: Gene editing and beyond [Video]. YouTube. <https://www.youtube.com/watch?v=4YKFw2KZA5o>
6. Negnevitsky, M. (2005). Artificial intelligence: A guide to intelligent systems (2nd ed.). Addison Wesley.
7. O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown.
8. Smith, G., & Rustagi, I. (2021, March 31). When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity. *Stanford Social Innovation Review*.