PRIVACY

Privacy

- The right and ability of individuals to control their personal information and decide how and when it is collected, used, and shared within the framework of legal and cultural norms.
- Privacy is a significant topic within the realm of legal and ethical issues.
- It involves the protection of an individual's personal information and their right to keep certain aspects of their life and identity private.

Personal Data vs Sensitive Personal Data

- **Personal data**: any piece of information that someone can use to identify, with some degree of accuracy, a living person.
  - e.g., name, address, phone number, email address, date of birth, financial details, and information related to work, education and hobbies.
- Personal data is also classed as anything that can affirm your physical presence somewhere.

Personal Data vs Sensitive Personal Data

- **Sensitive personal data** aka as **special category data**: a specific set of "special categories" that must be treated with extra security.
- It is a subset of personal data that requires higher levels of protection due to the potential harm if exposed.
- Includes highly confidential information that, if mishandled, could cause significant damage e.g.:
  - racial or ethnic origin; data related to a person's sex life or sexual orientation; and biometric data (where processed to uniquely identify someone).

Privacy

- We want to keep some (if not all) areas of our lives private.
- It is **our right** to do so.
- Though…
  - There seems to be a difference in how much we value our privacy, depending on which generation we belong to.
    - Social media generation
    - However, too, loyalty cards
  - See next slide for privacy preferences across generations.

Privacy Settings and Behaviours Across Age Groups

- Teens:
  - More likely to share personal information on social media.
  - Often keep profiles private and manage settings confidently.
- Young Adults (18-29):
  - Frequently click "agree" on privacy policies without reading.
  - Take actions to improve online data privacy.
- Middle-aged Adults (30-64):
  - Mixed behaviours: some read privacy policies, others don't.
  - Concerned about online privacy but not always proactive.
- Older Adults (65+):
  - Less likely to agree to privacy policies without reading.
  - Generally more cautious about online privacy.

Data Protection vs Freedom of Information

- When data was stored in paper form it was that much harder to work with.
- Today, massive amounts of data can be stored, accessed or moved/transferred at the click of a button.
- Two areas of law become of interest:
  - Data protection
  - Freedom of information …

Data Protection vs Freedom of Information

- Data protection
  - there should be **controlled** access to data about me
    - For privacy
- Freedom of information
  - I'd like to see/know what information the government/public authorities have
    - subject to certain exemptions

Privacy: Key Concepts

- Data Privacy
  - the protection of personal data and information from unauthorised access or misuse.
  - Laws that address this include the Kenya Data Protection Act (2019), Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States.

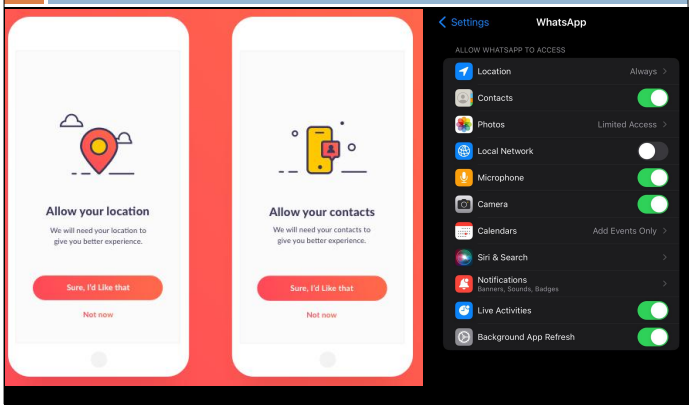
Privacy: Key Concepts

- Privacy Laws
  - Various countries and regions have enacted privacy laws to protect individuals' rights.
  - These laws define what constitutes personal data, how it can be used, and the penalties for violations.
    - E.g. they empower individuals with rights over their personal data:
      - Kenya's Data Protection Act, 2019, empowers Kenyan citizens to request access to their personal data held by a company.
      - The EU's GDPR empowers European citizens to request that a company deletes their stored data.

Privacy: Key Concepts

- Ethical Considerations
  - Privacy is not just a legal issue but also an ethical one.
  - It involves respecting individuals' autonomy and their right to control their personal information.
  - Essential ethical principles in this context include
    - consent
    - transparency
    - data minimisation ...

Privacy: Key Concepts



Privacy: Key Concepts

- Informed Consent
  - Users should be fully aware of **what** data is being collected, **how** it will be used, and the **implications** of that usage.
  - **Example**: An app requesting permission to access your contacts while explaining that this access is necessary for its core functionality, such as enabling you to invite friends.
- Informed Consent focuses on users agreeing to data collection with full knowledge of its purpose

Privacy: Key Concepts

- **Transparency**
  - Companies should clearly communicate their data practices and policies.
  - Example: A website providing an easily accessible privacy policy that details how user data is collected, used, and shared, including any third parties involved.
- Transparency mphasises **clear communication about data practices and policies** throughout the user experience.

Privacy: Key Concepts

- *Ethical Dilemma*
- *Is it ethical for a company to use personal data to personalise services if it improves user experience but also increases the company's profits?*

Privacy: Key Concepts

- Data Minimisation
  - Collect only the data necessary for a specific purpose.
    - E.g., an online shopping site only asks for your name and address during checkout.

Privacy: Key Concepts

- Technological Advances/New Technologies
  - Big Data, AI, the Internet of Things (IoT), 5G etc increase data accessibility and pose challenges to privacy.
  - They can collect and analyse vast amounts of personal data.
    - E.g., predictive algorithms analysing your online behaviour to make recommendations.
  - Ensuring privacy in these contexts is an ongoing concern.

Privacy: Key Concepts

- Other major concerns due to the proliferation of the internet:
- Online Privacy
  - Includes issues like tracking, data collection by websites and online services, cookies, and the use of personal information for targeted advertising.

Privacy: Key Concepts

- Other major concerns due to the proliferation of the internet:
- Social Media Privacy
  - Posting personal information on social media platforms can expose individuals to privacy risks.
  - Users often reveal personal information without considering the consequences.
    - Sharing geolocation data on social media while on vacation.
    - Posting vacation plans on social media can make you a target for burglars.

Privacy: Key Concepts

- Social Media Privacy (cont...)
  - Platforms' data collection practices and their use of personal information are subjects of debate.
  - Third-Party Apps connected to social media can access user data, sometimes without users realising.
    - A quiz app collecting users' Facebook data and selling it to advertisers.

Privacy: Key Concepts

- Healthcare Privacy
  - Laws such as the US' Health Insurance Portability and Accountability Act (HIPAA) govern the privacy of medical records and personal health information.
    - E.g., a healthcare provider cannot disclose a patient's medical history without their consent.

Privacy: Key Concepts

- Workplace Privacy
  - Employees have certain expectations of privacy in the workplace, but employers may monitor activities to varying degrees.
  - Balancing these interests is essential.

Privacy: Key Concepts

- Consumer Privacy
  - Companies often collect and use customer data for marketing and analysis.
    - E.g., concerns about the security of personal information when using mobile banking apps.
      - Safaricom collecting and using customer data for targeted marketing.
  - There are legal and ethical considerations around how they handle this data and whether individuals have consented to its use.

Privacy: Key Concepts

- Cultural Considerations
  - Community and Family
  - Kenyan culture has traditionally placed importance on communal living and family ties
  - This affects the boundaries of personal privacy.
    - E.g., family members may expect access to each other's personal information more readily than in some Western cultures.

Privacy: Key Concepts

- Surveillance
  - Government surveillance programs and the use of surveillance technologies (e.g., CCTV cameras, facial recognition) raise privacy concerns.
  - Balancing national security needs with individual privacy rights is a complex ethical and legal challenge.
    - Examples:
      - The debate over the use of facial recognition technology by law enforcement.
      - Unauthorised interception of text messages.

Mass surveillance

Scope creep ➔ mass surveillance

Mass/state/goverment surveillance: they can surveil certain persons for certain purposes...

Scope creep – now it seems to be ALL information about ALL people ALL the time.

Mass Surveillance

- The Panopticon
- Late 18th Century idea by Jeremy Bentham (English philosopher and social theorist).
  - One invisible warden in a central tower watches many individuals separated from each other.
  - To help manage correctional facilities by inducing good behaviour
    - the more people are watched, the better they behave.
      - the prisoners do not know who is being watched, thus they modify their behaviour accordingly.
- Inspired George Orwell's big brother's all seeing eye in "1984".

130

Prison San Vittore – Milan (built in 1880)

Source: thefunambulist.net

Mass Surveillance

- Bentham's Panopticon, and novels by HG Wells and Orwell, were futuristic fiction.
- Today it is a reality.
- Today both the state and individuals can use technology for mass surveillance: …
  - easy due to the prevalence of smart phones, CCTV in the malls and streets, speed cameras on the highways, Digital TV sets, ipads …

Mass Surveillance

- Organisations monitoring your communication
- What determines the content of what you share on your favourite social media network?
  - Probably influenced by the assumption that people are watching and judging you.
  - Others also assume you are watching and judging them.
  - So you all self-censor.

Mass Surveillance

- State surveillance
- Justification?
  - To curb terrorism
  - To tackle crime …
- How? …

Mass Surveillance

- The surveillance:
- Acts as a deterrent
  - Insidious (like the panopticon)
    - If we feel we are probably being watched we modify our behaviour accordingly.
- Provides information for investigation purposes.

Mass Surveillance Examples

- 2013: The NSA's mass surveillance programs, revealed by whistleblower Edward Snowden
- The programs, such as ***PRISM*** and ***XKeyscore***, involved the collection of massive amounts of electronic communications data, including emails and phone records (plus the ability to record and replay phone calls), from both U.S. citizens and non-citizens.
- Without judicial warrants;
- Using **phones + the internet** to carry out mass surveillance and data mining.
  - E.g. based on your internet searches and social networking data.

Mass Surveillance Examples

- China's Social Credit System
- A nationwide system that assigns scores to individuals and businesses based on their behaviour.
- Collects data from various sources, including financial transactions, social media activity, and public records, to assess citizens' trustworthiness.
- Individuals with high scores receive benefits, while those with low scores face restrictions.
- Basically mass surveillance and social control
  - it involves extensive data collection and monitoring of citizens' activities.

Mass Surveillance
Kenya

- In strategic areas in Nairobi;
- cameras that can recognise motor vehicle number plates
  - capture number plates of vehicles involved in traffic offences or crime (stolen/carjacked)

Mass Surveillance
Kenya

- To help the police force tackle crime, cameras installed in
  - Nairobi city
    - The Nairobi Integrated Urban Surveillance System project.
  - Mombasa

Mass Surveillance
Kenya

- Data is being collected, centralised and shared.
- **March, 2012**: the Communications Commission of Kenya (CCK) (now known as CA – Communications Authority):
  - Announced an increase in cyber security threats.
  - Declared the need for authorities to monitor digital communications.
- Service providers required to install NEWS (Network Early Warning System)
  - i.e. equipment used to monitor internet traffic.

Mass Surveillance
Kenya

- **December, 2012**
- The Integrated Population Registration System (IPRS)
- Developed for the Kenyan government by EDAPS, a Ukrainian firm.

Mass Surveillance
Kenya

- IPRS function: to collect and combine data from databases owned by various government agencies:
- All the following registers:
  - Birth & death, citizenship, ID card, aliens, passport, marriage & divorce, elections, tax, drivers, NSSF, NHIF (NB: in 2024, probably SHIF?), the Kenya National Bureau of Statistics.

(Privacy International, 2019)

- The running of this system was *allegedly* subcontracted to a foreign country.
- *PS: It was hacked…*

Surveillance Activities
Other Examples

- **March, 2013**
- The Ministry of Information PS announces that mobile service providers were blocking at least 300K "hate" SMSs **daily**.
- Ostensibly to prevent violence in the 4th of March elections;
- service providers had installed software to
  - detect messages containing particular words (e.g. kill)
  - automatically flag them off for further scrutiny and potential blocking.

Surveillance Activities
Other Examples

- April 2014
- The Kenyan government proposes the *Umoja Kenya Initiative*, a universal single registration system
  - Activated when a child is born
  - Stored in a national digital database.
- Collect:
  - Individuals' biometric details
  - other personal information collected
    - E.g. name, age, relatives' identities, location and assets owned.

Surveillance Activities
Other Examples

- **Aims:**
- To identify people with fake identification documents.
- To provide one digital ID
  - to streamline registrations
    - E.g. voter, national ID, NHIF, NSSF, KRA, commercial/business related.
  - rather than have different cards for each.

Surveillance Activities
Other Examples

- **July 2015:** Wikileaks allegations:
- The Kenyan government wanted to procure a Remote Control System tool;
  - to remote hack and control target devices.
- Requested a foreign intrusion malware company (HackingTeam) to shut down a blog.
- This would serve as a Proof of Concept.
- If successful they would win the contract to supply surveillance tools.

Surveillance Activities
Other Examples

- A presidential directive that names of people living with HIV, including school age children be collected.
- The Kenya Legal & Ethical Issues Network and others sued the government in December 2016…
- **December, 2016**
- The High Court in Nairobi declared this directive unconstitutional.

Surveillance Activities
Other Examples

- Argued such a list violated the Constitution's:
- Article 31
  - the right to privacy
- Article 53(2)
  - the "child's best interests are of paramount importance in every matter concerning the child."

Surveillance Activities
Other Examples

- January 2017, CA announced their plan to implement a **device management system:**
- Ostensibly to identify fake and stolen devices.
- In reality: a spy system to monitor digital communications:
  - a third party (a foreign firm) connects to mobile service providers' routers
  - To snoop on private communication data
    - SMS, call and mobile money transfer data.

Surveillance Activities
Other Examples

- The Consumer Federation denounced it as:
  - against the Constitution
  - exposing service providers to lawsuits for breach of confidentiality.

Surveillance Activities
Other Examples: Huduma Number

- January 2019
- The president signed into law amendments to the Registrations of Persons Act.
  - Basically about introducing the National Integrated Identity Management System (NIIMS)
  - i.e., a biometric ID card with a unique ID number
    - aka the "Huduma Namba".
- For all Kenyans and all foreign residents.

Surveillance Activities
Other Examples: Huduma Number

- Previously all that was needed as a unique identifier was finger/thumb prints.
- This amendment added DNA information;
  - E.g. hand and ear lobe geometry, retina, iris and voice patterns in digital form.
- Also more location info
  - e.g. land reference number, plot and house number and GPS coordinates.

Surveillance Activities
Other Examples: Huduma Number

- **March 2019**
- The National Integrated Identity Management System (NIIMS) launched.
- Aim: one card merging information from multiple documents.
- These numerous implementations of modern technology are a good thing.
- **Right?**

Surveillance Activities
Other Examples: Huduma Number

- Once more, massive amounts of personal data was being collected, centralised and shared.
- YET!...
- Kenya had yet to adopt data protection legislation around these activities.
  - The project lacked adequate data protection measures and oversight.

Data Processing vs Privacy

- The constitution enshrines our right to privacy.
- But pre-November, 2019 there was no law to specifically give it effect.
- No data protection law ➔ an individual's personal information can be abused by those that obtain it.

Data Processing vs Privacy

- A Data Protection Bill has existed in various forms since…
- 2012…!!
- The Kenyan Data Protection Bill (2019) was the latest version.
- At long last (November 8, 2019) the president signed it into law.

Surveillance Activities

- Previously :
  - No data protection law
  - No data protection agency/authority.
- Yet all this data about an individual stored in one database.
- The problem being there was no law to protect it.

Surveillance Activities
Other Examples: Huduma Number (cont) …

- Also:
- Is the practice and spirit of it such initiatives as the Huduma No. from a genuine place?
- If we are not to find this system suspect, we must be assured that the government has our interests at heart.
- cf the Aadhar Number…

India

- The **Aadhaar** number was initially publicised as a **voluntary** service.
- However citizens without this number were denied certain crucial services
  - E.g. collection of payments for those on welfare.

Privacy vs Secrecy/Surveillance

- Data privacy is a right.
- Data protection laws are not normally seen as important
  - is data privacy as important as violation of your human rights or freedom of expression?
- In many countries, privacy and surveillance rarely seen as important in the larger context.
  - We are inured by the oft repeated message:
    - Surveilling us is beneficial to us due to increasing security threats.

Privacy vs Secrecy/Surveillance

- Do we need data protection laws?
- If a man in the middle attack happens then your data is open to everyone.
  - Turkey – 2016. Super sensitive information about its citizens (names, their locations etc) found on a torrent file.
- So what? You have nothing to hide, right?

Nothing To Hide

Video clip from *The Circle* (2017)

Privacy vs Secrecy/Surveillance

- National IDs registration requires information on our location of origin.
- Enables whoever is interested to figure out your tribe/ethnicity.
- Your data can be weaponised (used against you) e.g. it can be used to track you down.
  - E.g. voter registration
    - to verify that you are on the voter roll, type in your ID no.
    - You get your name and voting locale.
    - Nice but then so does anyone else with your ID number

Privacy vs Secrecy/Surveillance

- E.g. during elections:
  - personalised text messages sent to citizens in some counties asking them why they had not registered as voters.
  - chiefs had people's numbers and their locations and would visit them to enquire and encourage them to vote.
- Implication: personal data is not secure and mass surveillance is carried out.

Privacy vs Secrecy/Surveillance

- Should someone working at one parastatal have access to your data at another parastatal?
- How about KRA having across the board information about you?
  - E.g. KRA attempts to access M-Pesa transaction records "to catch tax cheats".

Privacy vs Secrecy/Surveillance

- Wanting privacy is **NOT** akin to you having something to hide.

  Privacy is NOT Secrecy.
- It is the ability to control the collection, use, sharing etc of your personal data …

Privacy vs Secrecy/Surveillance

- You probably have nothing to hide.
- However, you desire the ability to have your own space, free thoughts, free speech etc. …
- … without surveillance.
- Governments may not want this, as they wish to prevent dissidence.
- Self censorship also kills creativity and innovation.

Privacy vs Secrecy/Surveillance

- In most countries, governments are allowed to
  - tap private conversations and
  - access personal data
- As long as
  - there is a valid reason and
  - permission from the courts.

Privacy vs Secrecy/Surveillance

- However some seem to require citizens to give up their rights in the name of ***national security***.
- **Judicial oversight** discourages the government from abusing this privilege
  - even if fighting terrorism.

Data Protection Issues

- Having nothing to hide shouldn't justify lack of data protection legislation.
- As a human, you have **autonomy…**
- This is a fundamental right.
  - Basically, do what you want, when you want, without hindrance / feeling watched.

Why should we care?

- The information / digital age is powered by information
- Technological advances have led to massive amounts of our data being out there.
- Corporations and governments worldwide hunger for this information
  - This data is sorted and you are profiled based on the data.
  - Worse: automated decisions could be made based on this data.

Why should we care?

- We have little/no ability to control what is done to our data if there are no legal mechanisms in place.
- Your digital persona can easily affect your physical persona negatively
  - Persuasion through ads
  - Harassment e.g. cyberbulling/stalking
  - Blackmail eg ransomware
  - Discrimination
    - Information in the wrong hands can be dangerous

Why should we care?

- Information is a priceless commodity that we give out for free.
- Why not sell it?
  - Watch Stuart Lacey's TEDxBermuda talk titled: "The Future of Your Personal Data - Privacy vs Monetization"
  - *https://www.youtube.com/watch?v=Jlo-V0beaBw*

Why should we care?

- Big data firms seem to have more power than governments.
- Governments want to regain their power
- A country may have exponential growth in e-commerce (as Kenya does).
  - Many citizens run their businesses on FB, Instagram, e-commerce platforms like Jumia and Amazon.
- No legislation to protect data meant people's sensitive data was online but unprotected.

Why should we care?

- Data breaches
  - E.g. instances of millions of FB accounts being hacked.
  - FB has a lot of data about a lot of people…
- GDPR: To transact with businesses based in EU countries/trade we must have data protection laws.
  - Without them we miss out on trade opportunities.

Why should we care?

- EU countries have the power to hold corporations to account
  - e.g. telling FB that it's standards are not up to par with their legal requirements
- This protects their citizens' data/privacy.
- Governments without such legislation may have no standing to do the same.

Mass Surveillance & The Absence of Identified Unjust Threats

- Usually there is no identified unjust threat in the case of almost everybody that is subjected to mass surveillance.
- There is no identified unjust threat meaning individuals are often monitored without any specific evidence or suspicion that they are involved in wrongdoing.
- This can lead to infringement on privacy rights and civil liberties without justified cause and has several implications …

Mass Surveillance & The Absence of Identified Unjust Threats

- **Presumption of Innocence**:
  - People are treated as potential threats based on generalised criteria rather than actual behaviour.
  - This undermines the principle of presuming innocence until proven guilty.
- **Broad and Indiscriminate Monitoring**:
  - Mass surveillance systems typically collect data from large populations without targeting specific individuals.
  - This can result in the monitoring of law-abiding citizens alongside those who may pose a legitimate threat.

Mass Surveillance & The Absence of Identified Unjust Threats

- **Chilling Effect:**
  - The lack of a clearly identified threat can create a chilling effect.
  - This is where individuals alter their behaviour due to the fear of being watched, even if they have done nothing wrong.
- **Erosion of Trust:**
  - When surveillance is pervasive without justifiable cause, it can erode trust between citizens and authorities
  - This leads to feelings of paranoia and alienation.

Privacy in Surveillance

Video: Person Of Interest

Surveillance and Proportionality Requirements

- In their work, Kira Vrist Rønn and Kasper Lippert-Rasmussen discuss the concept of surveillance and its proportionality requirements
- They emphasise that surveillance measures must be balanced against individual rights and freedoms.
- They argue that surveillance should be justified by a **legitimate aim** and must be **necessary** and **proportionate** to that aim.
- This means that the level of intrusion into personal privacy should be minimised and only used when no less intrusive alternatives are available.

Vrist, K., & Lippert-Rasmussen, K. (2020). *Out of Proportion? On Surveillance and the Proportionality Requirement* Ethical Theory and Moral Practice, February 2020

Understanding Privacy Rights and Reasonable Expectations

Privacy rights (if they do exist) do not require that no one know our personal information, but rather that those who become privy to such information do not share it with others inappropriately (i.e. share it with those who are not entitled to it).

- Gaukroger, C

Data Protection

Legal, Ethical and Human Rights Issues

Data Protection Issues

- Having massive amounts of personal information → profiling → denial of services.
- Concerns:
  - Legal
  - Ethical
  - Human rights

Data Protection

Legal Issues

Data Protection
Legal Issues

- For a long time there has been no data protection law/legal framework to support the government collecting huge amounts of personal data.
  - Fortunately the constitution did protect citizens (Article 31).
- E.g. as of 2019, a popular Kenyan service provider + a local bank teamed up to provide overdrafts to subscribers …

Data Protection Legal Issues

- When you opt in, one of the T&Cs is:
  - You allow them access to the information the Integrated Population Registration System (IPRS) system holds about you.
    - IPRS was developed for the **Kenyan government** (NOT private corporates!!).
- Ditto other businesses with apps that offer credit services …

Data Protection Legal Issues

- How and why did **private entities** have access to such potent data**?**
- Because there was no legal framework governing the IPRS.
- The **Registration of Persons Act** allows collection of data but doesn't discuss it's protection.
- The government should not serve private business interests; it should serve the citizens.

Data Protection Legal Issues

- Can malicious entities get access to this information then?
- With access even to DNA info?
- Can I be tracked using my eye/facial recognition data from all the CCTV cameras?

Data Protection Legal Issues

- Danger of private communication data held by CA being exposed;
- **January, 2017:** The CA website hacked by *AnonPlus* who placed their manifesto on the homepage
  - They promised to "*defend freedom of information, freedom of the people and emancipation of the latter from the oppression of media*".

Data Protection
Legal Issues

- Errors in personal data
  - From e.g. data storage/transfer glitches or hacks
- If my data (e.g. DNA data) is corrupted:
  - wrongful arrest (mistaken id)?
  - denial of services?
    - both by government or private entities
    - E.g. your credit history is ruined due to automated decisions
      - living in a certain neighbourhood …

Data Protection
Legal Issues

- Privacy violations
  - A lender app accesses your phone book and sends messages shaming you to your contacts
  - Today Apple notifies you when an app wants to access your contacts, location, photos etc.
  - It wasn't always so.
    - Without your consent apps would:
      - access your address book (almost 1/5 of all its apps),
      - track your location (2/5 of the apps) and
      - have this data stored unencrypted (> 2/5 of the apps).
- identity theft aka identity fraud

Data Protection

Ethical Issues

Data Protection
Ethical Issues

- **How ethical are the following:**
- Compulsory collection of sensitive personal data (DNA, GPS coordinates etc) for the sake of collection?
- State "honesty" in explaining its data collection?
  - Is the passing of amendments to certain laws done with transparency / accountability / integrity in mind?

Data Protection
Ethical Issues

- **How ethical are the following:**
- The state having considerable insight into our lives?
- The state enabling others (private corporations/individuals) to have insight into our lives
  - e.g. through security breaches)?

Data Protection
Ethical Issues

- **How ethical are the following:**
- Treating humans as their data (am I my data)?
  - "ok" and profitable for businesses but…
  - … governments actions should not be driven by commercial interests/profit margins
- Cambridge Analytica – data used to breach the democracy of at least two developed nations.
  - How sovereign are we?

Data Protection

Human Rights Issues

Data Protection
Human Rights Issues

- **Right to privacy**
- The state/its official organs having massive amounts of data can be dangerous
- Your information can be weaponised
  - E.g. genocide is made easy…
  - Marginalisation (resource allocation)
  - Wrong profiling – you are of religion X therefore you are a terrorist
    - (automated decision making)

Data Protection
Human Rights Issues

- Right to privacy
- The data collector may not be a government officer
  - they may simply be hired contractors trained with no notion of privacy
- cf
  - Huduma namba;
  - political SMSs sent to your "private" cellphone number

Data Protection
Human Rights Issues

- **Right to privacy**
- Once more:
- Privacy is a **fundamental** human right.

Data Protection
Human Rights Issues

- **Right to Dignity**
- Violation of dignity:
  - The state + private corporations too aware of your activities/life
- Your have a right to your freedom and security
  - Being treated as a human.
  - Automated decision making violates that.

Data Protection
Human Rights Issues

- **Right to Equality**
  - Article 27 of the constitution.
  - No discrimination …
  - Regardless of gender/ethnicity …

Data Protection
Human Rights Issues

- **Right to Equality**
- ***No discrimination …***
  - Location information:
  - We are told information is collected to provide services.
    - What about the homeless? Refugees? People living in domestic violence shelters?
    - No services for them?

Data Protection
Human Rights Issues

- **Right to Equality**
  - ***Regardless of gender/ethnicity …***
    - Why fill these details in government forms then?
    - Provision of DNA information can be used to trace your ancestors' origins.

Data Protection
Human Rights Issues

- **Right to Equality**
- Not being treated equally = torture
  - A database for People Living with HIV.
    - To serve what purpose?
  - Automated decision making ➔ profiling ➔ discrimination

Data Protection
Human Rights Issues

- **Right to Equality**
- Not being treated equally = torture
  - Say you are not in the database …
    - No government services?
      - Infringes on your right to welfare payments, right to health care, right to vote …
      - cf Aadhaar number

Is Data Protection Legislation Necessary?

- Mass surveillance implies data on individuals is generated, collected and processed regardless of their being involved (or suspected to be involved) in criminal activities.
- This "*distorts the burden of proof principles, leads to an unaccountable increase in power, and has a chilling effect on individual action and the exercise of free speech.*"

(Kiprono, 2018) …

Is Data Protection Legislation Necessary?

- When individuals are under constant surveillance, there may be a presumption of guilt or suspicion, shifting the burden of proof from the prosecution to the defense.
  - Mass surveillance can create an environment where individuals are treated as potential suspects until they can prove their innocence.
- This chilling effect on freedom of expression
  - Knowing that they are being monitored, individuals may self-censor their online activities and communications out of fear of being targeted or labeled as a potential threat.

Is Data Protection Legislation Necessary?

- Good governance requires the state to respect its citizens right to express their opinions freely.
  - E.g. in exposing corruption, injustice and malpractices against consumers
    - Buyer Beware.
  - Fighting terrorism should not be an excuse for bad governance.
    - Not the right way to fight terrorism.
    - Identify the root problem.
    - What makes someone become a terrorist/radicalised?
    - Could it be marginalisation/discrimination?