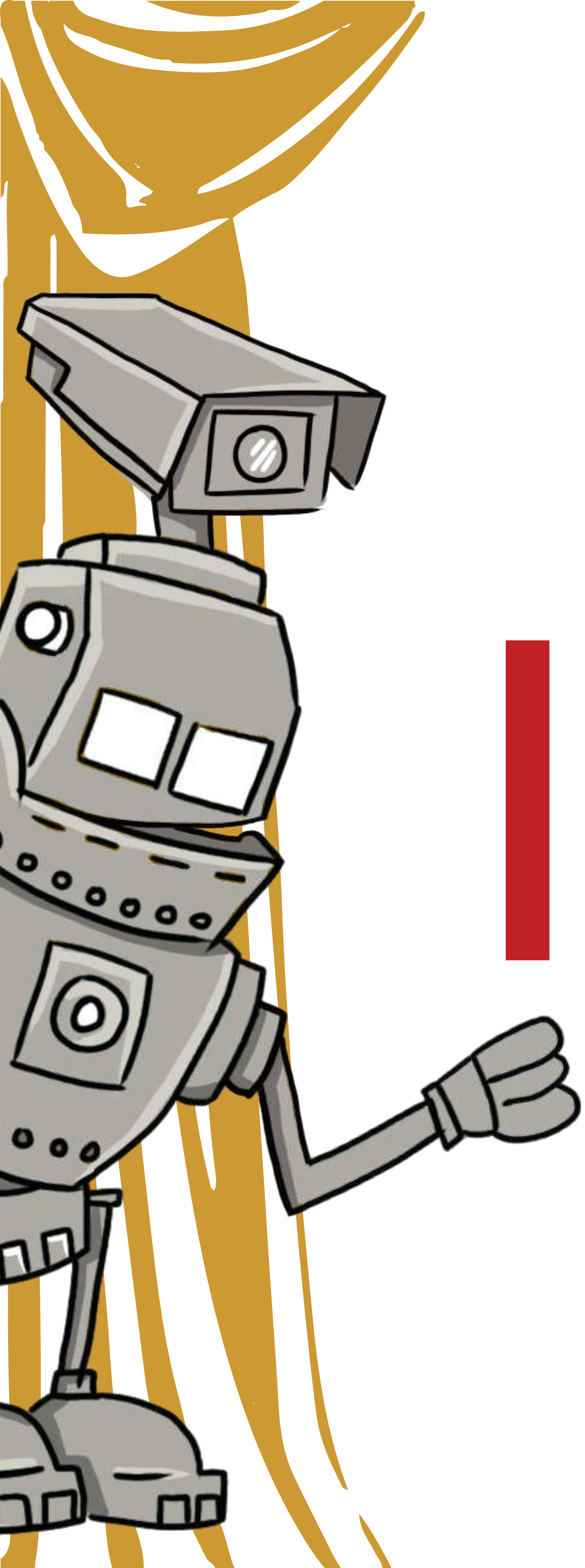


UNVEILING PRIVACY IN THE AI ERA:

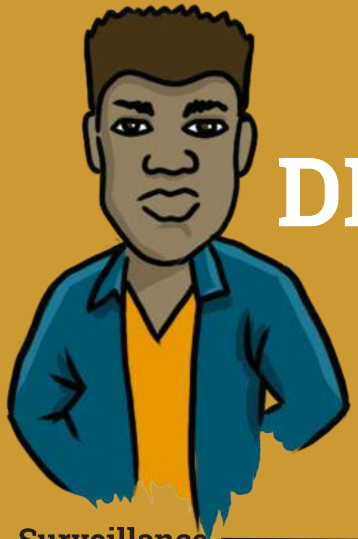
NAVIGATING SURVEILLANCE, ETHICS, AND EQUITABLE SOLUTIONS

Strathmore University

Centre for Intellectual Property and Information Technology Law

UNVEILING PRIVACY IN THE AI ERA:

NAVIGATING SURVEILLANCE, ETHICS, AND EQUITABLE SOLUTIONS



DEFINITIONS

Surveillance

It involves the observation, recording and categorization of information about people, processes and institutions. It has also been defined as the collection and analysis of information about populations in order to govern their activities.

Privacy

It has been defined as the right to be let alone, or freedom from interference or intrusion. Information privacy has been defined as the right to have some control over how your personal information is collected and used.

Importance of Privacy in the Digital Era

Privacy in the digital era is of paramount importance due to the significant impact that technology and the internet have on our lives. Here are some key reasons why privacy is crucial in the digital age:

Personal security: Privacy safeguards individuals from potential threats such as identity theft, cyberstalking, harassment, and other forms of digital crimes. Without adequate privacy measures, people's personal information and sensitive data become vulnerable to malicious actors who can misuse it for nefarious purposes.

Data protection: In the digital age, vast amounts of data are generated and collected by various organizations, including governments and corporations. Protecting individuals' privacy ensures that this data is handled responsibly and ethically, preventing unauthorized access or data breaches that could lead to devastating consequences for individuals and society as a whole.

Autonomy and individual freedom: Privacy allows individuals to exercise control over their personal information and make autonomous decisions without the fear of judgment, discrimination, or manipulation. It fosters a sense of independence and empowers individuals to express themselves freely without the fear of constant surveillance.

Trust in digital services: Trust is the foundation of any successful digital service or online interaction. Users are more likely to engage with technology and share their information when they believe their privacy is protected. By respecting privacy, businesses and institutions can build trust with their users and customers, enhancing long-term relationships.

Intellectual property protection: Privacy is essential for safeguarding intellectual property rights. Creators and innovators need assurance that their ideas and creations won't be stolen or misused, which is critical for fostering innovation and creativity in the digital world.

Democracy and free speech: In a digital society, the free flow of information and ideas is vital for the functioning of democracy. Privacy protects individuals engaged in political discourse or activism from surveillance, censorship, or reprisals, ensuring that diverse voices can participate freely.

Avoidance of discrimination and profiling: Without proper privacy protections, individuals may be subjected to discriminatory practices based on their personal information, such as race, religion, gender, or other characteristics. Privacy regulations help mitigate such risks and promote fairness and equality.

Innovation and progress: Striking a balance between privacy and data access can lead to ethical data-driven innovation. Respecting privacy while leveraging data for research and development can yield significant societal benefits without compromising individuals' rights.

General Privacy Challenges in the Age of AI / Risks and Challenges in AI-driven Data Processing

The age of AI brings with it numerous benefits and opportunities, but it also introduces several privacy challenges and risks associated with AI-driven data processing. Some of the key challenges include:

Data Privacy and Security: AI systems rely heavily on vast amounts of data to train and improve their performance. However, this creates privacy concerns as sensitive and personal data could be used without proper consent or security measures, leading to potential data breaches or unauthorized access.

Data Bias and Fairness: AI algorithms may unintentionally perpetuate biases present in the training data. When these algorithms are used for decision-making processes like hiring or lending, it can lead to unfair outcomes and discrimination, raising ethical and privacy concerns.

Re-identification and De-anonymization: AI technologies can potentially re-identify individuals from supposedly anonymized data sets by cross-referencing them with other available information. This undermines the promise of anonymity and poses risks to individuals' privacy.

Invasive Surveillance: AI-powered surveillance technologies, such as facial recognition systems and behavioral analysis tools, can significantly erode privacy by constantly monitoring and tracking individuals without their knowledge or consent.

Data Over-collection: AI-driven applications often collect large amounts of data, sometimes beyond what is necessary for the intended purpose. This practice raises concerns about data minimization and puts individuals' privacy at risk.

Informed Consent and User Awareness: Obtaining informed consent from users can be challenging, especially when users are unaware of how their data is being used or lack a clear understanding of AI and its implications on their privacy.

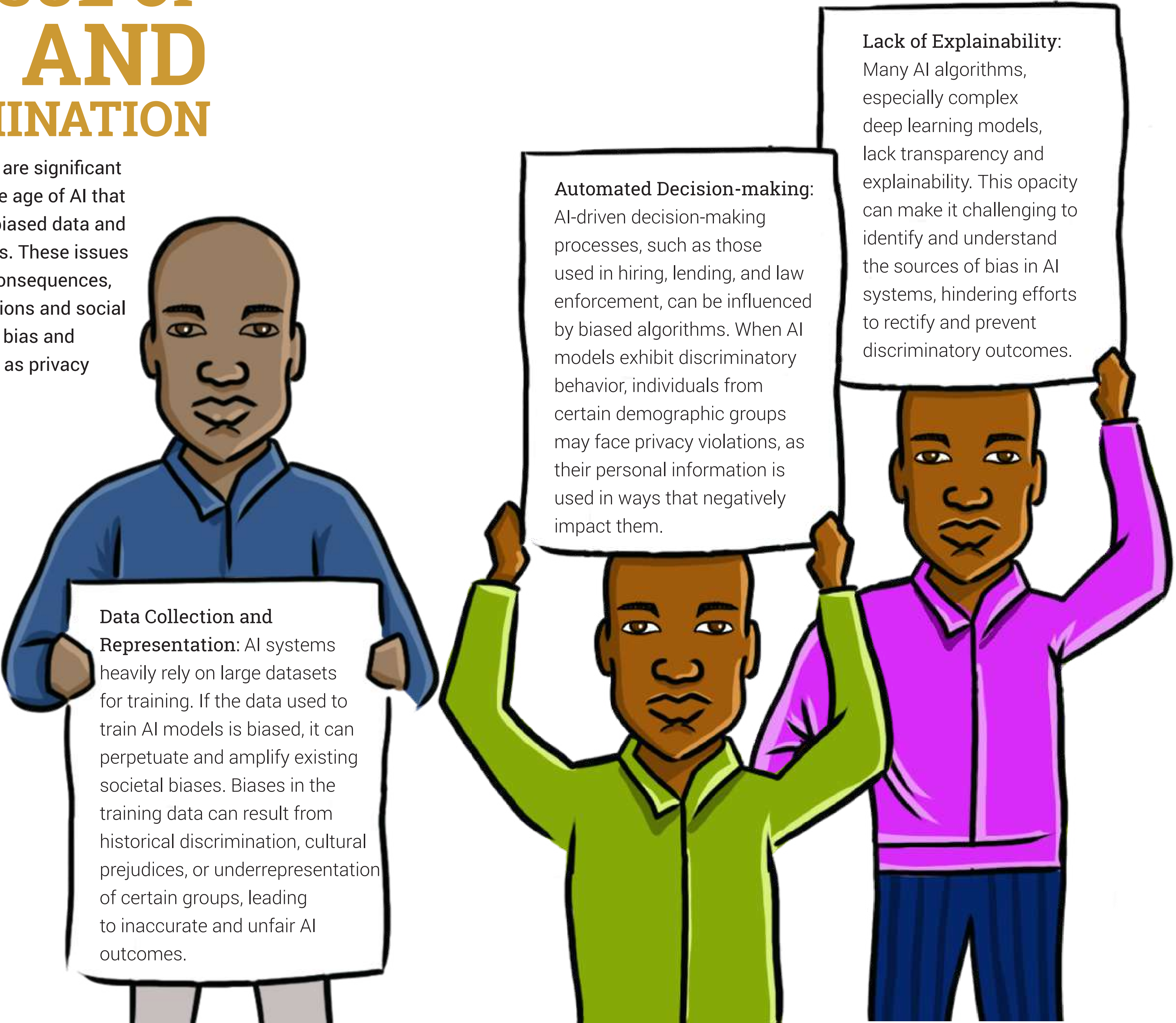
Adversarial Attacks: AI models can be vulnerable to adversarial attacks, where malicious actors intentionally manipulate data inputs to deceive the AI system or compromise its integrity. Such attacks can lead to privacy breaches and misinformation.

Third-party Sharing and Profiling: AI systems, particularly in the realm of online advertising and social media, may share user data with third parties for profiling and targeted advertising. This can lead to privacy violations and manipulation of users' behavior.

Transfer of Data across Borders: The use of AI may involve the transfer of data across international borders. Divergent privacy regulations in different countries can create challenges in ensuring consistent privacy protection for users.

THE ISSUE OF BIAS AND DISCRIMINATION

Bias and discrimination are significant privacy challenges in the age of AI that arise due to the use of biased data and algorithms in AI systems. These issues can have far-reaching consequences, leading to privacy violations and social inequalities. Here's how bias and discrimination manifest as privacy challenges in AI:



Data Collection and Representation: AI systems heavily rely on large datasets for training. If the data used to train AI models is biased, it can perpetuate and amplify existing societal biases. Biases in the training data can result from historical discrimination, cultural prejudices, or underrepresentation of certain groups, leading to inaccurate and unfair AI outcomes.

Automated Decision-making: AI-driven decision-making processes, such as those used in hiring, lending, and law enforcement, can be influenced by biased algorithms. When AI models exhibit discriminatory behavior, individuals from certain demographic groups may face privacy violations, as their personal information is used in ways that negatively impact them.

Lack of Explainability: Many AI algorithms, especially complex deep learning models, lack transparency and explainability. This opacity can make it challenging to identify and understand the sources of bias in AI systems, hindering efforts to rectify and prevent discriminatory outcomes.

Unintentional Privacy Violations: Biased AI systems might lead to unintended privacy violations when they disproportionately target or surveil certain groups. For example, biased facial recognition systems may wrongly identify individuals and invade their privacy.

Exclusion and Inequality: Discriminatory AI systems can exacerbate social inequalities and exclude certain groups from opportunities and services. This exclusion can lead to privacy concerns, as some individuals may be denied access to essential services or subjected to targeted discrimination.

Lack of Consent and Control: Biased AI systems can make decisions about individuals without their consent or understanding. When people are unaware of how their data is used to fuel biased algorithms, they have limited control over their personal information and privacy.

THE ISSUE OF BIAS AND DISCRIMINATION

Feedback Loops: Biased AI systems that provide unequal opportunities and outcomes can create feedback loops that perpetuate and reinforce existing biases. For example, biased hiring algorithms may continue to favor certain demographics, leading to an underrepresentation of other groups in the workforce

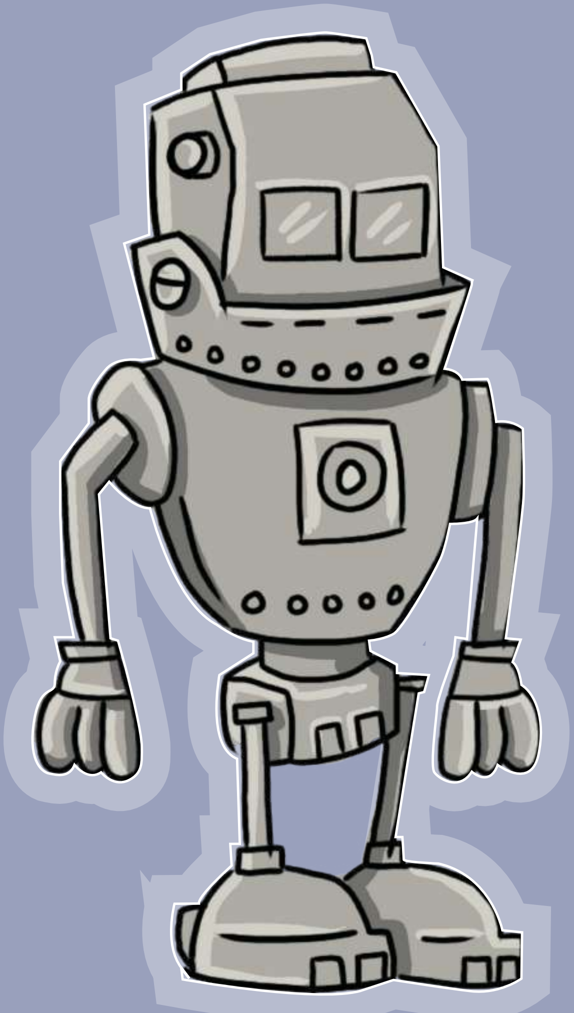
The Issue of Job Displacements for Workers

Job displacement for workers is a significant privacy challenge in the age of AI, primarily due to the following reasons:

Sensitive Employment Data: As AI-driven automation and machine learning technologies replace certain job functions, workers may face job losses or changes in their employment status. This can involve sensitive personal information, such as job performance evaluations, career history, and financial details. If this information is not handled with proper privacy measures, workers' personal and professional lives could be adversely affected.

Data Breaches and Third-party Sharing: Job displacement often involves sharing employee data with third-party service providers or contractors handling the transition to AI-based systems. If proper data protection protocols are not in place, there is a risk of data breaches, leading to the exposure of workers' private information to unauthorized parties.

Algorithmic Decision-making: In some cases, AI algorithms may be used to determine job retention or severance decisions. If these algorithms are not transparent or explainable, workers may not fully understand the reasons behind their job displacements, leading to concerns about fairness and privacy.

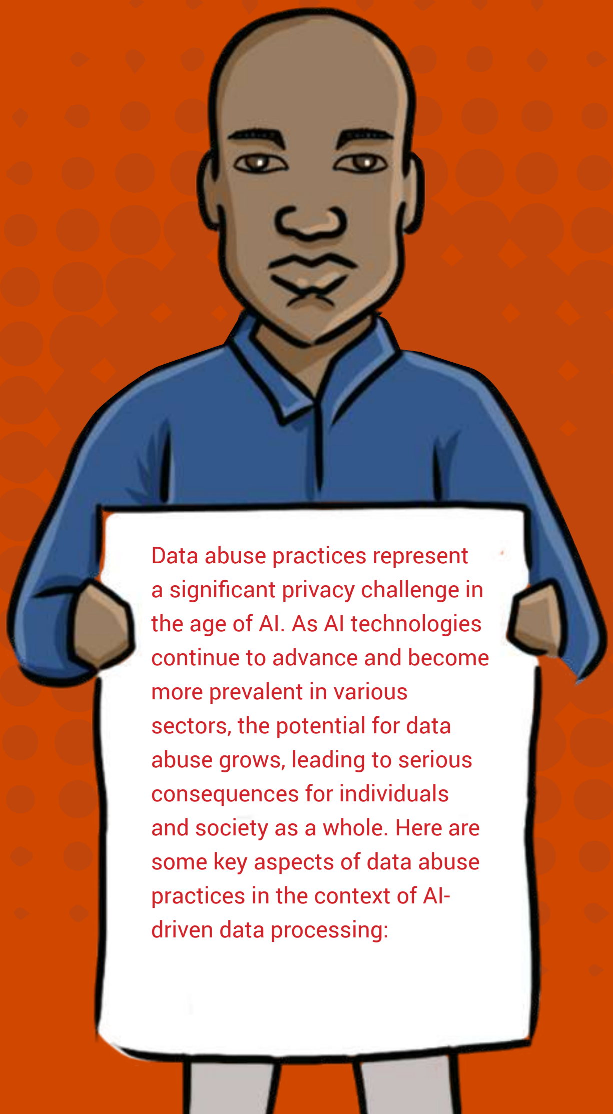


Discrimination and Bias: AI algorithms can inadvertently perpetuate biases present in historical employment data, leading to discriminatory job displacement practices. This could disproportionately affect certain groups of workers based on factors like age, gender, race, or disability, raising concerns about privacy and equal opportunities.

Lack of Control over Personal Information: Workers facing job displacement may find that their personal information is used and shared in ways they have little control over. This lack of control can erode individuals' trust and confidence in how their data is being handled during the job transition process.

Data Retention and Deletion: After job displacements, employers must handle workers' personal data appropriately. Retaining this data for extended periods without a clear purpose can be a privacy concern, especially if workers are unaware of how their information is being used.

The Issue of Data Abuse Practices



Data abuse practices represent a significant privacy challenge in the age of AI. As AI technologies continue to advance and become more prevalent in various sectors, the potential for data abuse grows, leading to serious consequences for individuals and society as a whole. Here are some key aspects of data abuse practices in the context of AI-driven data processing:

Unethical Data Collection: Data abuse occurs when organizations collect personal information without explicit consent or through deceptive means. AI systems often rely on vast datasets to function effectively, and unethical data collection practices may lead to the accumulation of sensitive data without individuals' knowledge or approval.

Data Monetization without Consent: In some cases, organizations may collect user data and then monetize it by selling or sharing it with third parties without the knowledge or consent of the individuals involved. This practice infringes upon user privacy and autonomy over their personal information.

Manipulative Profiling: AI-driven data processing enables detailed profiling of individuals based on their online activities, preferences, and behaviors. This information can be used to create targeted advertising or content that may manipulate user choices and behaviors without their awareness.

Algorithmic Discrimination: AI algorithms can inadvertently perpetuate biases present in the data they are trained on. This can result in discriminatory practices, such as biased hiring decisions, loan approvals, or law enforcement profiling, which disproportionately affect certain groups and infringe upon their privacy rights.

Excessive Data Retention: AI systems may store vast amounts of data beyond what is necessary for their intended purpose. This excessive data retention can increase the risk of data breaches and unauthorized access, putting individuals' privacy at risk.

Surveillance and Tracking: AI-powered surveillance technologies can lead to constant monitoring and tracking of individuals' activities, both online and offline. This invasive surveillance compromises personal privacy and can lead to a chilling effect on free expression and behavior.

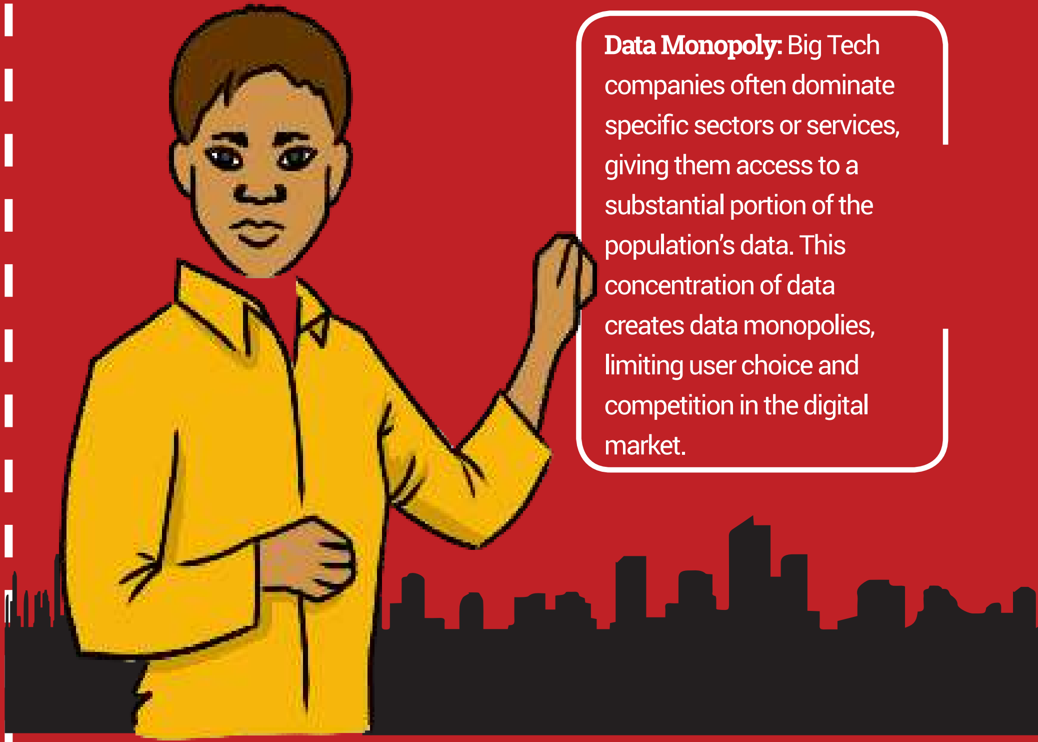
Inadequate Data Security: Mishandling and inadequate security measures can result in data breaches and leaks, making personal information vulnerable to exploitation and misuse.

AI-generated Misinformation and Deepfakes: AI technologies can be used to generate convincing fake content, such as deepfake videos and audio, which can be employed to spread misinformation, manipulate public opinion, and compromise individuals' privacy and reputation.

Cross-referencing Data from Multiple Sources: AI systems can combine data from various sources to build comprehensive profiles of individuals, potentially revealing sensitive information that individuals may not want to share.

The Power of Big Tech on Data

The power of Big Tech companies on data is a significant privacy challenge in the age of AI. Big Tech companies, such as Google, Facebook, Amazon, Apple, and Microsoft, have amassed vast amounts of data from their users, giving them unprecedented control over personal information and data-driven technologies. This power presents several privacy concerns:



Data Monopoly: Big Tech companies often dominate specific sectors or services, giving them access to a substantial portion of the population's data. This concentration of data creates data monopolies, limiting user choice and competition in the digital market.

Data Collection and Profiling: These companies collect a wide range of data from various sources, including user interactions, browsing behavior, location data, and social connections. Through sophisticated AI-driven algorithms, they create detailed user profiles for targeted advertising and other purposes, which can feel intrusive and erode privacy.

Opaque Data Practices: The data practices of Big Tech companies are often complex and opaque, making it challenging for users to understand what data is being collected, how it is being used, and who it is being shared with.

Informed Consent: Obtaining informed consent from users can be problematic, as the lengthy terms and conditions documents are often difficult to comprehend, leading to users unknowingly giving up significant amounts of personal data.

Potential for Misuse: The extensive data repositories of Big Tech companies can be misused, intentionally or unintentionally, compromising user privacy and leading to incidents like the Cambridge Analytica scandal.

Influence on Public Discourse: The control over data gives these companies significant influence over public discourse, leading to concerns about privacy in the context of political and social issues.

Cross-platform Tracking: Big Tech companies often have a vast network of services and platforms. They can track users across multiple platforms and devices, accumulating extensive user profiles that allow them to gain insights into users' lives and behavior.

Lack of Data Portability and Interoperability: Users may find it challenging to transfer their data between different platforms or services due to a lack of data portability and interoperability, limiting their control over their personal information.

Data Breaches and Security Concerns: The vast repositories of user data held by Big Tech companies become lucrative targets for hackers and other malicious actors, leading to concerns about data breaches and data security.

Limited Regulation and Oversight: Due to their global reach and complexity, regulating the data practices of Big Tech companies poses challenges for governments and regulatory bodies, potentially leaving users' privacy vulnerable.

Data Collection and Use by AI Technologies

AI technologies heavily rely on data collection and use to perform various tasks and improve their performance over time. Here's how data collection and use by AI technologies work:

Data Collection: AI systems require large amounts of data to train their models effectively. This data can come from various sources, such as:

Sensor Data: IoT devices and sensors generate data that AI systems can use for tasks like environmental monitoring, smart home automation, and healthcare applications.

User Interactions: AI systems collect data from user interactions with digital platforms, including clicks, searches, likes, comments, and other forms of engagement.

Text and Language Data: AI models that process natural language rely on text data from sources like websites, social media, and documents.

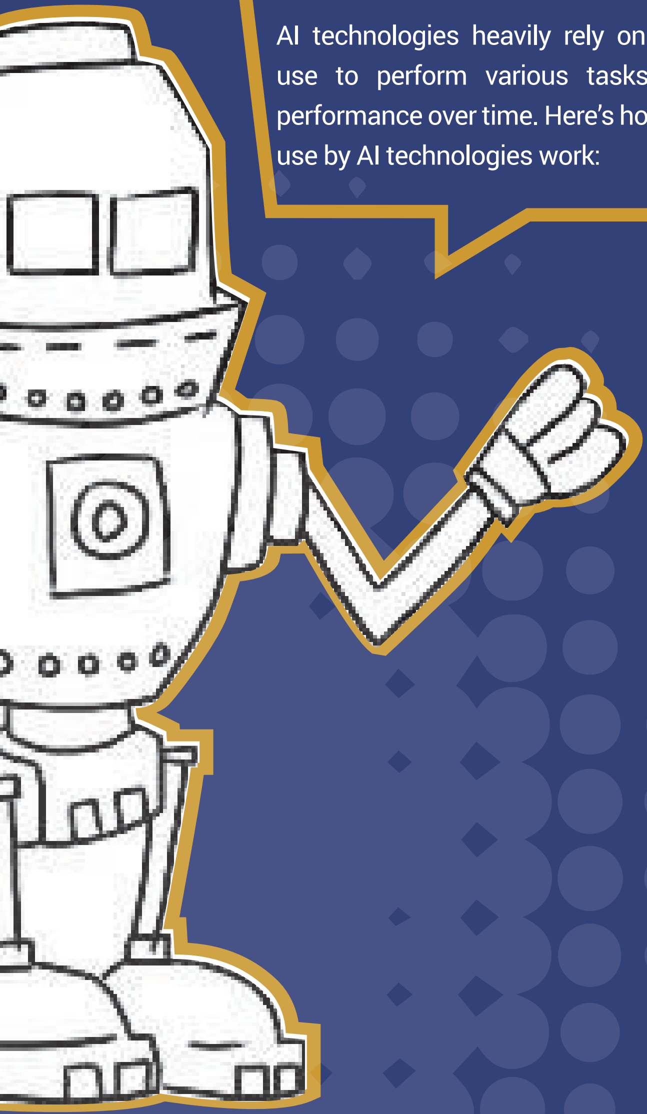


Image and Video Data: Computer vision AI systems use images and videos for tasks like object recognition, image captioning, and facial recognition.

Data Preprocessing: Once collected, the data undergoes preprocessing, which involves cleaning, filtering, and organizing it to make it suitable for training AI models. This step ensures that the data is in a usable format and free from errors or inconsistencies.

Data Annotation: For supervised learning, where AI models are trained with labeled data, human annotators label the collected data to provide ground truth or reference for the AI model to learn from. For example, in image recognition, annotators label images with corresponding object names.

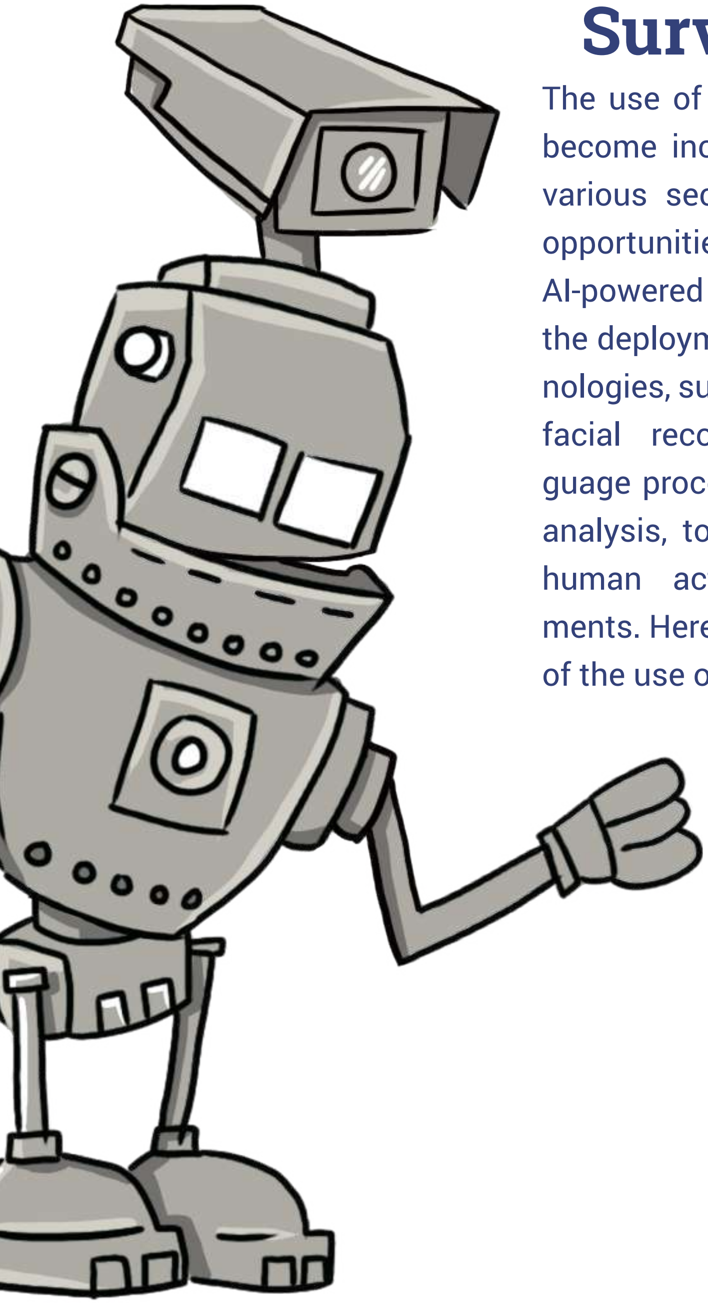
Training the AI Model: The preprocessed and annotated data is then used to train the AI model. The AI algorithm processes the data, identifies patterns, and adjusts its internal parameters to optimize its performance on the task at hand. This training process is often iterative and can be computationally intensive.

Continuous Learning and Adaptation: AI models can continue to learn and adapt even after the initial training phase. They may receive feedback from users' interactions and make updates to improve their performance over time, a process known as online learning or incremental learning.

Data Use in Inference: Once trained, AI models are deployed to perform specific tasks in real-world scenarios. During inference, the trained model processes new, unseen data to make predictions, generate insights, or provide recommendations.

User Personalization: AI technologies often use collected data to personalize user experiences, such as showing tailored content, product recommendations, or targeted advertisements based on individual preferences and behavior.

Privacy Concerns: The extensive data collection and use by AI technologies raise privacy concerns. Users may worry about the security and confidentiality of their data, as well as the potential for misuse or unauthorized access to their personal information.



The Use of AI in Surveillance

The use of AI in surveillance has become increasingly prevalent in various sectors, presenting both opportunities and challenges. AI-powered surveillance involves the deployment of advanced technologies, such as computer vision, facial recognition, natural language processing, and behavioral analysis, to monitor and analyze human activities and environments. Here are some key aspects of the use of AI in surveillance:

Enhanced Monitoring and Analysis: AI-driven surveillance systems can process vast amounts of data from video feeds, sensors, and other sources in real-time. This enables more efficient and comprehensive monitoring of public spaces, traffic, retail stores, airports, and other areas.

Facial Recognition: AI-powered facial recognition technology can match faces against databases of known individuals, raising concerns about privacy, civil liberties, and the potential for misuse.

Improved Object Recognition: AI algorithms can accurately recognize and track objects, faces, and vehicles in video streams. This capability enhances the ability to identify individuals and objects of interest in surveillance footage.

Predictive Analytics: AI can analyze data patterns to identify potential security threats or unusual behavior, enabling proactive responses to prevent or mitigate security incidents.

Public Safety and Crime Prevention: AI surveillance can aid law enforcement in tracking criminals, locating missing persons, and preventing criminal activities, potentially enhancing public safety.

Remote Monitoring: AI-driven surveillance allows remote monitoring of locations, reducing the need for constant physical presence and providing real-time alerts for suspicious activities.

Biases and Misidentifications: AI facial recognition systems have shown biases, misidentifications, and inaccuracies, particularly concerning minority groups. These errors can lead to wrongful arrests or discrimination.

Legal and Regulatory Challenges: The rapid deployment of AI surveillance has outpaced the development of robust legal and regulatory frameworks, leading to uncertainty regarding its proper use and potential abuses.

Traffic Management: AI can optimize traffic flow and enhance road safety by analyzing real-time traffic data, identifying congested areas, and adjusting traffic signals accordingly.

Privacy and Ethical Concerns: The use of AI in surveillance raises significant privacy and ethical concerns. Widespread surveillance could infringe on individuals' right to privacy and lead to mass surveillance and tracking of innocent citizens.

Lack of Transparency and Accountability: The lack of transparency in how AI surveillance systems work can be concerning. People being monitored may not know when, where, or how their data is being collected, used, and stored.

Chilling Effect on Society: Mass surveillance can create a chilling effect on free speech and expression, potentially stifling dissent and inhibiting social progress.

AI-related Privacy Concerns: Examples

AI-related privacy concerns arise from the increasing use of artificial intelligence technologies that rely on vast amounts of data. Here are some examples of privacy concerns related to AI:

Facial Recognition and Surveillance:

Facial recognition technology powered by AI can be used for mass surveillance, tracking individuals' movements without their knowledge or consent. This raises concerns about invasion of privacy and the potential for misuse by government agencies or private entities.

Biased Algorithms:

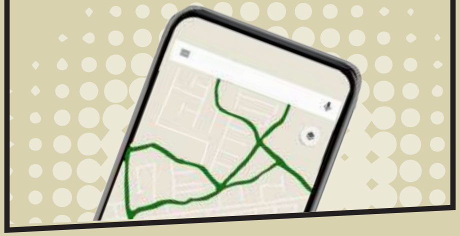
AI algorithms can inadvertently perpetuate biases present in the training data. For example, an AI-powered hiring tool might discriminate against certain demographics due to biased historical hiring practices in the training data.

Data Breaches and Security:

AI systems collect and process massive amounts of data, making them potential targets for hackers and data breaches. If these breaches occur, sensitive personal information could be exposed, leading to privacy violations.

Location Tracking and Behavioral Analysis:

AI technologies can track users' location and behavior to offer personalized services or targeted advertisements. However, this raises concerns about constant monitoring and the potential for surveillance capitalism.



Deepfakes and Misinformation:

AI can be used to create convincing deepfake content, such as videos or audio clips, that can deceive individuals or manipulate public opinion, leading to privacy breaches and misinformation.

Healthcare Data Privacy:

AI is being used to process medical data, leading to concerns about patient privacy and the potential for data breaches containing sensitive health information.

Lack of Explainability:

Some AI models, particularly deep learning algorithms, lack transparency and are challenging to explain. This opacity can make it difficult for users to understand how their data is being used to make decisions that affect them.

Virtual Assistants and Voice Data:

Virtual assistants like Siri, Alexa, or Google Assistant process voice data to understand and respond to user commands. Concerns arise about these companies listening to and storing voice recordings for analysis and improvement, potentially compromising user privacy.

Predictive Policing:

AI-powered predictive policing systems analyze historical crime data to anticipate future crime hotspots. However, this raises concerns about potential over-policing in certain communities and the erosion of civil liberties.

Ad Targeting and User Profiling:

AI-powered algorithms track user behavior to create detailed profiles for targeted advertising. This can lead to personalized but intrusive ads and the potential for manipulation.

Internet of Things (IoT) Devices:

AI is increasingly integrated into IoT devices, raising privacy concerns about data collection, processing, and sharing in the connected environment.

Best Practices and mitigation measures for Privacy and Data Protection in AI

To ensure privacy and data protection in AI, adopting best practices and mitigation measures is crucial. Here are some recommended strategies:

Privacy by Design: Implement privacy considerations from the inception of AI projects. Embed privacy features into the design and architecture of AI systems to minimize risks to user data.

Data Minimization: Collect and retain only the necessary data required for the intended purpose of the AI application. Avoid unnecessary data collection to limit potential privacy risks.

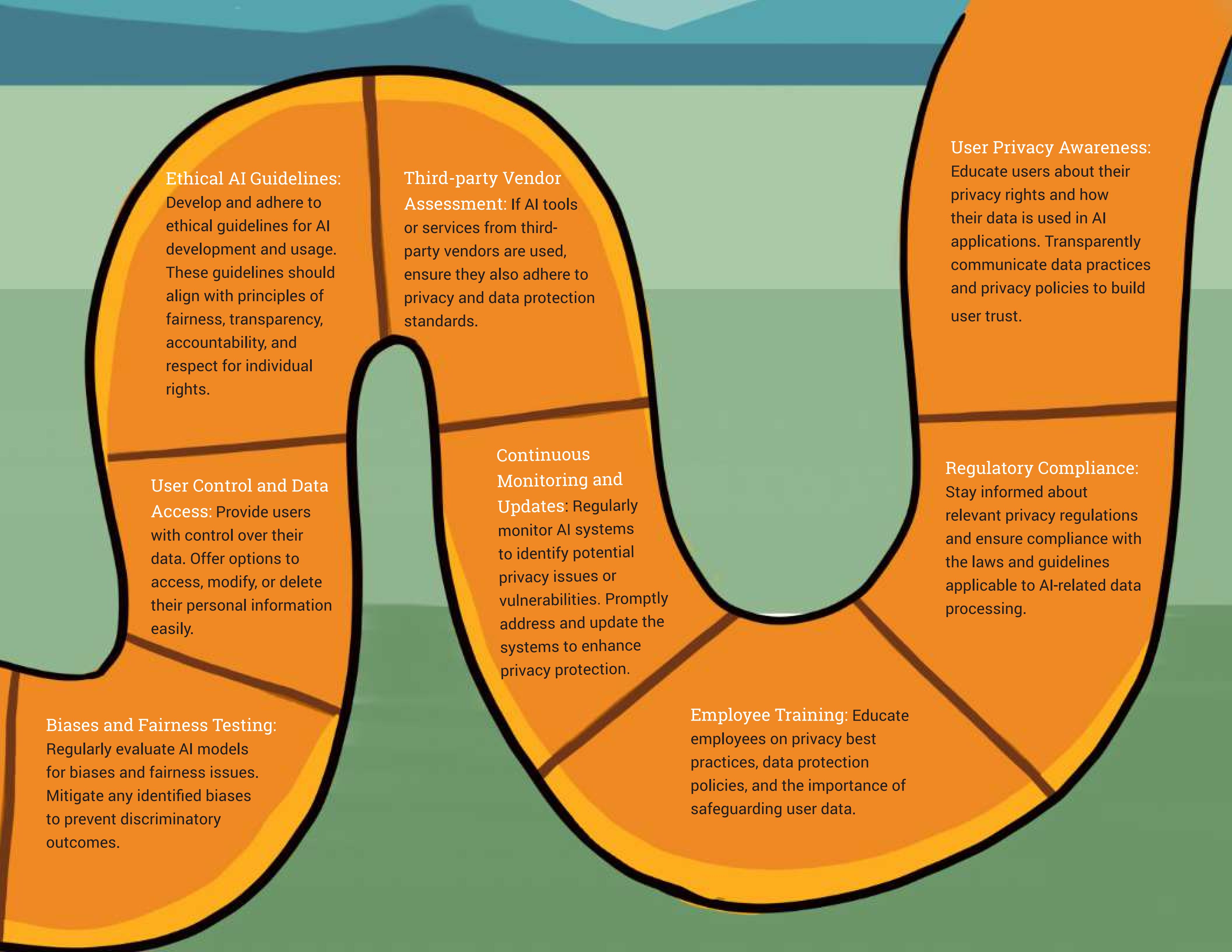
Informed Consent: Obtain explicit and informed consent from individuals before collecting and processing their data. Clearly explain how their data will be used and provide easy-to-understand options to opt-out.

Anonymization and Pseudonymization: Anonymize or pseudonymize personal data whenever possible, reducing the risk of re-identification and protecting individual identities.

Transparency and Explainability: Ensure AI algorithms are transparent and provide explanations for the decisions they make. Users should have visibility into how their data is used and how AI-generated insights are derived.

Regular Data Audits and Assessments: Conduct regular privacy impact assessments (PIAs) and data protection audits to identify potential risks and ensure compliance with privacy regulations.

Secure Data Storage and Transfer: Implement robust security measures to protect data at rest and in transit. Use encryption and secure protocols to safeguard sensitive information.



Biases and Fairness Testing: Regularly evaluate AI models for biases and fairness issues. Mitigate any identified biases to prevent discriminatory outcomes.

User Control and Data Access: Provide users with control over their data. Offer options to access, modify, or delete their personal information easily.

Ethical AI Guidelines: Develop and adhere to ethical guidelines for AI development and usage. These guidelines should align with principles of fairness, transparency, accountability, and respect for individual rights.

Third-party Vendor Assessment: If AI tools or services from third-party vendors are used, ensure they also adhere to privacy and data protection standards.

Continuous Monitoring and Updates: Regularly monitor AI systems to identify potential privacy issues or vulnerabilities. Promptly address and update the systems to enhance privacy protection.

Employee Training: Educate employees on privacy best practices, data protection policies, and the importance of safeguarding user data.

Regulatory Compliance: Stay informed about relevant privacy regulations and ensure compliance with the laws and guidelines applicable to AI-related data processing.

User Privacy Awareness: Educate users about their privacy rights and how their data is used in AI applications. Transparently communicate data practices and privacy policies to build user trust.

Kenya's Digital Transformation and AI Policy Landscape

Kenya is making significant strides in positioning itself within the digital economy, despite the absence of a formal national AI strategy.

Blockchain and AI task force:

established to explore the potential of these emerging technologies established.

Data Protection Act:

enacted in 2019, this legislation establishes a robust framework for safeguarding personal data, providing individuals with control over their information.

Digital Economy Blueprint:

aligning with the broader Digital Economy Blueprint for Africa

Kenya Digital Master Plan (DMP) 2022-2032:

This comprehensive blueprint identifies 20 flagship programs, spanning digital infrastructure, government services, digital skills, and digital enterprises, alongside an overarching policy, legal, and regulatory framework.

Investments in AI research and development:

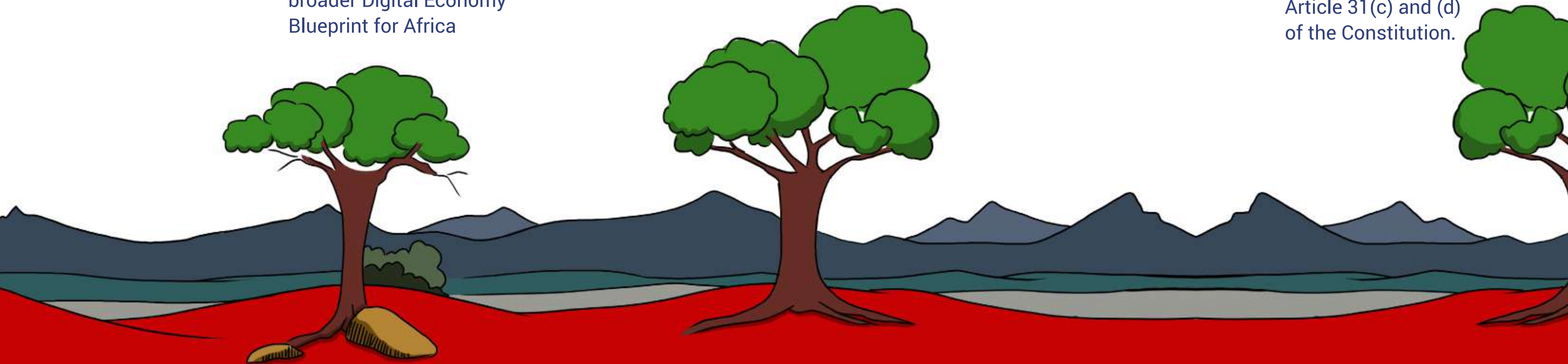
an accumulated investment of Sh13 billion (US$120 million) over the past decade

Public Consultation portal of the Communications Authority of Kenya:

a systematic process for public participation in policy-making

Data Protection Act (DPA):

aimed to safeguard personal data and uphold the right to privacy, aligning with Article 31(c) and (d) of the Constitution.



Office of the Data Protection Commissioner (ODPC):

was established in 2020 and joined the Global Privacy Assembly (GPA) in 2022, connecting with over 130 data protection authorities worldwide.

Introduction of additional regulations in 2021 and 2022 :

to enhance privacy and support its digital economy, including measures to address unethical debt collection practices and digital credit provider regulations.

Highlighting algorithmic transparency:

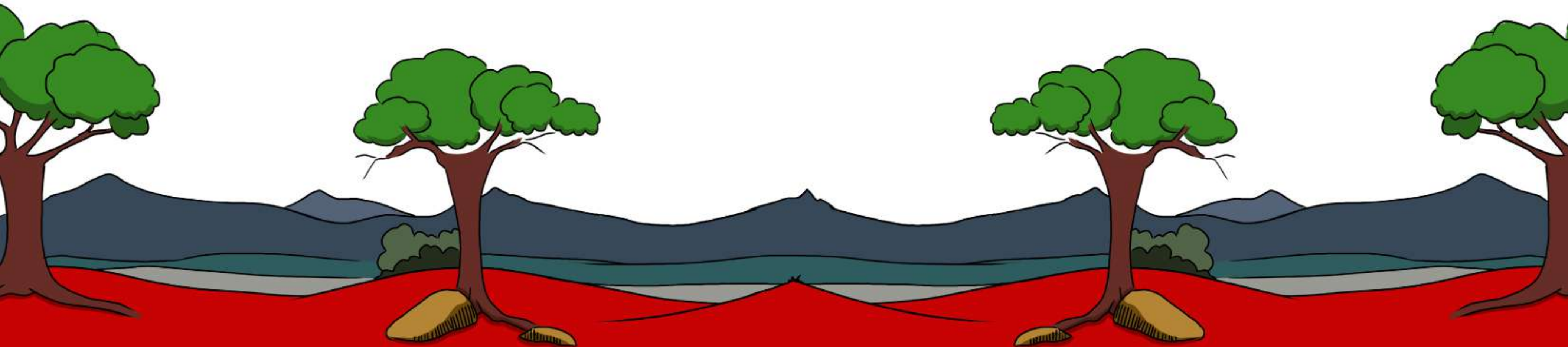
requiring data controllers and processors to inform data subjects about automated individual decision-making and provide meaningful information about the underlying logic

Biometric registration:

On the 29th of September, the government issued an official press statement indicating the postponement of the forthcoming inauguration of the Maisha Namba and Digital ID ecosystem, initially slated for October 2, 2023, under the auspices of His Excellency President William Ruto. A revised launch date will be communicated in due course. Concurrently, the process of soliciting public input and engaging with stakeholders concerning the Maisha Namba and Digital ID ecosystem is actively progressing across the nation.

Facial recognition:

the Kenyan National Police Service launched a system in 2018 to detect vehicles involved in crimes through CCTV cameras and Automatic Number Plate Recognition (ANPR).



African Approaches to Protecting Privacy in the Age of AI

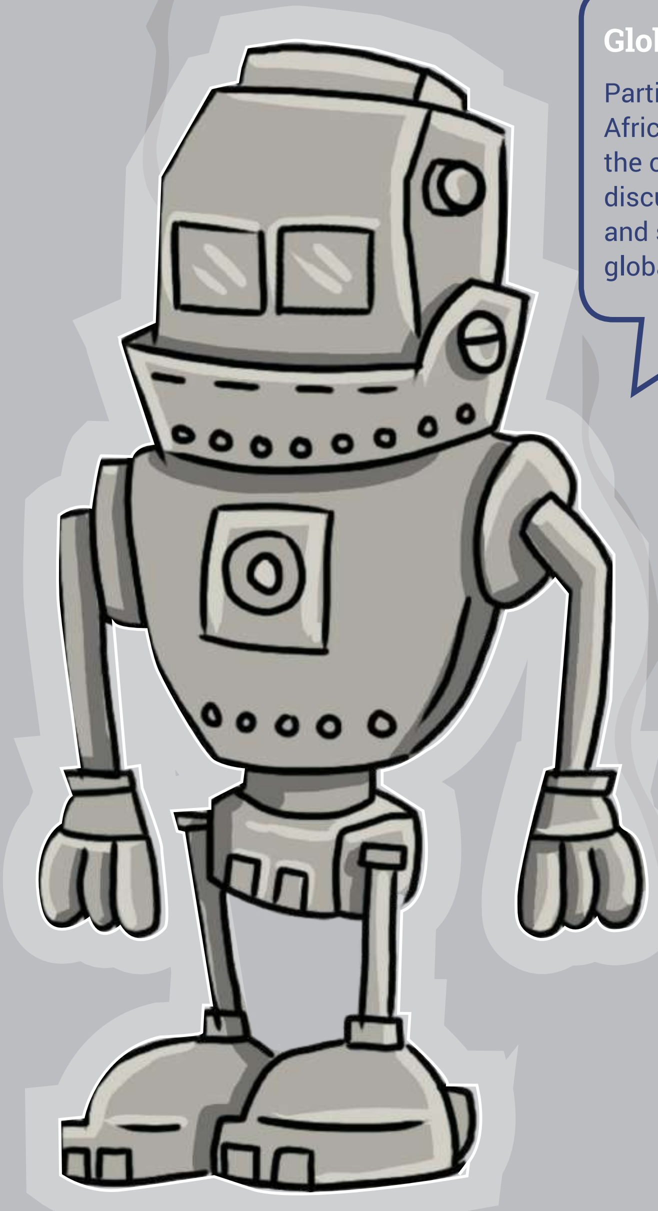
Global approaches and initiatives can provide valuable insights and frameworks to guide African countries in their efforts to enhance privacy and data protection in the realm of artificial intelligence. Some of these approaches include:

General Data Protection Regulation (GDPR):

Enacted by the European Union, has had a significant influence on global privacy standards. Its emphasis on individual data rights, consent, and data protection principles serves as a valuable reference point for African nations as they work to strengthen their own privacy regulations.

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework:

Aligning with these principles can guide African countries in crafting privacy regulations that resonate with their cultural and societal contexts while upholding fundamental data protection values.



Global Privacy Assembly :

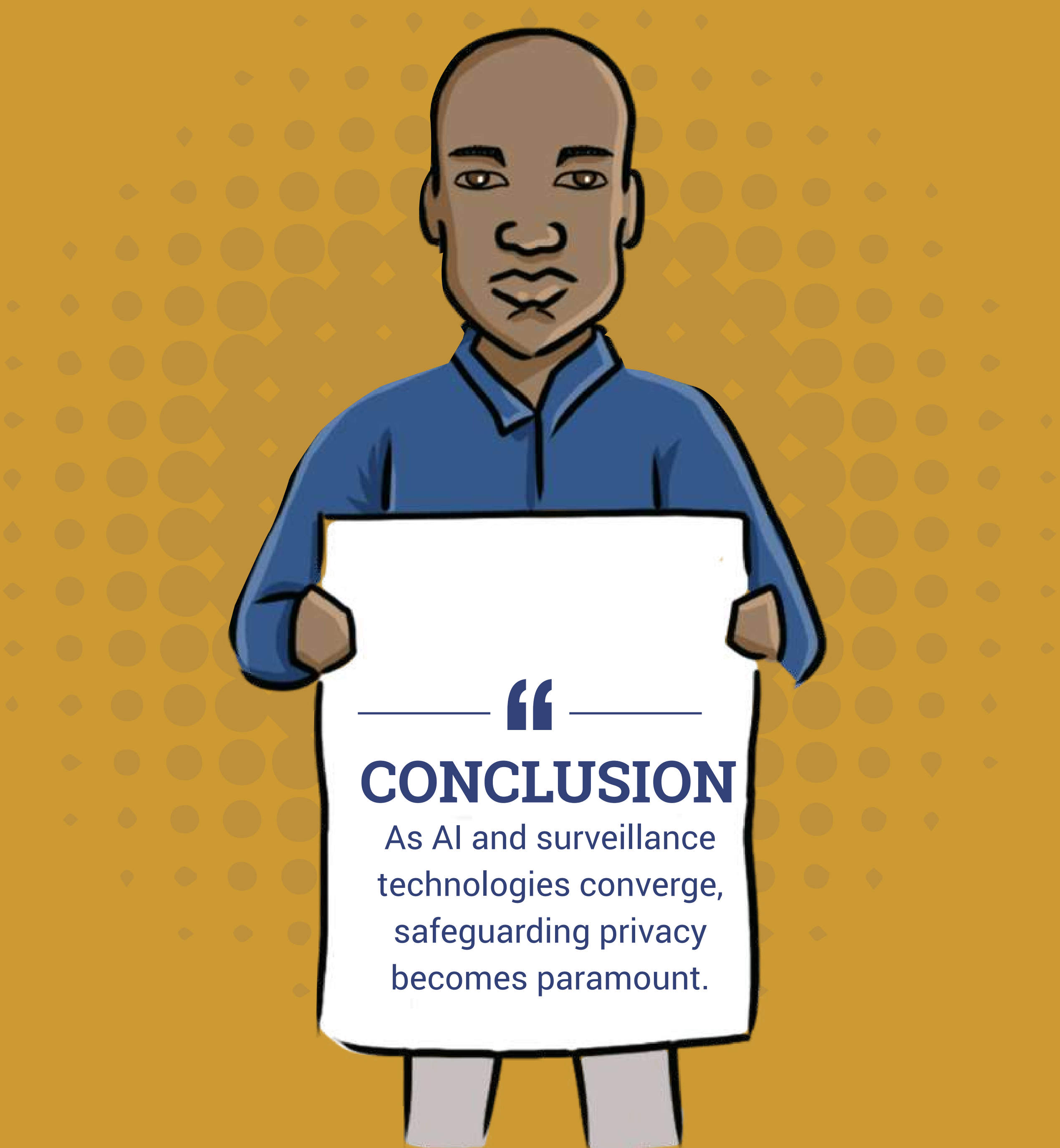
Participation in this assembly offers African data protection authorities the opportunity to engage in discussions on privacy challenges and share best practices with their global counterparts.

Privacy-Enhancing Technologies (PETs) :

Hold great promise for bolstering data protection in Africa's AI landscape. Embracing these technologies can enhance the overall privacy posture of AI applications in Africa.

Promotion of public awareness and education :

African nations must empower individuals to make informed decisions about their privacy rights in the context of AI technologies.



CONCLUSION

As AI and surveillance technologies converge, safeguarding privacy becomes paramount.

This study was made possible by a grant provided by the International Development Research Center (IDRC). We thank the organization for their continued support.

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

The information in this infographic was compiled by Doreen Abiero and proofread by Dr. Angeline Wairegi and Valerie Kutima. It was designed by Gloria Muthoka.

The icons used in this infographic were sourced from https://www.flaticon.com

Strathmore University

Centre for Intellectual Property and Information Technology Law