DATA PROTECTION IN KENYA

Policy brief examining the current state of data protection in Kenya and the development of a consolidated framework to provide for data protection principles.

About KICTANet

KICTANet is a multi-stakeholder platform for people and institutions interested and involved in ICT policy and regulation. It was was formed as part of a World Summit of Information Society (WSIS) project under catalyzing Access to ICTs in Africa (CATIA) initiative in 2003. The network aims to act as a catalyst for reform in the ICT sector in support of the national aim of ICT enabled growth and development.

Objectives of the Network are:

1. To improve the effectiveness of ICT policy and regulatory processes by expanding support for ICT initiatives, providing support for member's actions and audience for member's ideas.
2. Facilitate effective dissemination channels regarding ICT policy and regulatory processes to keep everyone updated on what is going on in the sector
3. Provide access to varied and multiple resources/skills
4. Link organisations and networks working at the community level to those specialised and working in the broader political space

POLICY BRIEF:
DATA PROTECTION IN KENYA

This policy brief examines the current state of data protection in Kenya and recommends the development of a consolidated framework to provide for data protection principles.

Email us: info@kictanet.or.ke
Website: www.kictanet.or.ke
Twitter: @kictanet

Design and Layout: Amos Ochieng/PixelsKenya

TABLE OF CONTENTS

Acronyms

GDPR	General Data Protection Regulation (of the European Union)
ICT	Information and communications technology
IPRS	Integrated Population Registry Services
MSMEs	Micro, small and medium enterprises
NEMIS	National Education Management Information System
TIMS	Transport Integrated Management System

Acknowledgement

KICTANet is grateful to listers on the platform- their discussions on Kenya's data economy inspired different aspects of data protection discussed in this paper.
We are extremely grateful to Grace Mutung'u and Mercy Mutemi who researched and wrote the paper with assistance from Francis Monyango and guidance from Victor Kapiyo and Grace Githaiga. Special mention to listers S. M Muraya, John Walubengo, Barrack Otieno, Gideon Rop and Gabriel Warigi who offered feedback that enriched the research.

Additional comments were also received from our partners, in particular Estelle Masse, and Billy Goodman of AccessNow; and Richard Wingfield and Sheetal Kumar of Global Partners Digital. Editing was done by Grace Githaiga .

This research was made possible through grants from our partners Ford Foundation and AccessNow.

Executive Summary

In the last two decades in Kenya, mobile communications and internet connectivity have rapidly increased. With these developments, the country has also developed a data economy. The data economy is the wealth and resources created from collection and processing of data. It is the cornerstone of the fourth industrial revolution which uses digital technologies to carry out processes, be they physical, digital, or biological. Key features of this revolution are data-driven decision making, creation of new products, services and innovation.

Data-driven decision making has various effects on society which could result in more efficient distribution of resources such as water, health and emergency services. However, collecting and using data has direct implications for people's right to privacy, which is constitutionally protected in Kenya. Inappropriate use of data can also propagate existing inequalities as only those whose data is available are included in planning and decision making. In other instances, data may be used to discriminate against particular groups. This may be deliberate or from automated decision making, where on the input given, the system makes erroneous or a rights demoting decision(s).

Kenya has a significant data economy spanning both public and private sector. The government through the Integrated Population Register Services (IPRS) has been digitalising analogue paper records of the public. It has also centralised databases containing millions of personal records from several registries. These include details on birth, death, immigration and passports, marriage, elections, tax, drivers, education, health insurance and social security. Recent additions to the project include the National Education Management Information System (NEMIS) through which details of all school going children have been captured in a central database.

Others examples of such indices are the Independent Electoral and Boundaries Commission (IEBC), which is a biometric database containing close to 20 million voters' data the National Social Security Fund (NSSF) register, National Hospital Insurance Fund (NHIF) register and the Kenya National Bureau of Statistics (KNBS).

The country is in a biometric craze with various private organisations either piloting or implementing voice, fingerprint, face and iris recognition systems. The rationale for the private databases is to curb fraud. Some of these private entities, for instance banks and mobile network operators (MNOs), have access to the centralised government database for verification of identity documents. However, the trends seem to be movement from validation of documents to authentication of people's identity. Hence everywhere in Kenya, public and private bodies are seeking to update their databases. It has become common to be asked for a new photo or primary documents even where there is one already on record.

There are a number of laws that require confidentiality of data. These include the Official Secrets Act; Children's Act; HIV and AIDS Prevention and Control Act; Witness

Protection Act; Banking Act, Credit Reference Bureau Regulations and Capital Markets Act; Access to Information Act; and the Public Archives and Documentation Service Act. Others are the Kenya Information and Communications Act (KICA); Private Security Regulation Act; and the Elections (Technology) Regulations, 2017. Together with professional ethics and pronouncements of the courts, these laws regulate aspects of processing of data in specific cases. However, they do not comprehensively cover all instances of data processing in our modern reality. For example, educational institutions collect personal data of their students but they are not required to protect the data from unauthorised access and use. Online platforms that people use to access internet services for example Facebook and Twitter are not subject to data protection licence conditions under KICA. There have also been previous legislative attempts to come up with a data protection law which did not materialise as they were not introduced in Parliament.

This has therefore created policy concerns from economic, fairness, rights and political data perspectives. From an economic perspective, the key concern is that the government digitalization project is without a policy or legal framework. The government collects massive amounts of personal data in the absence of a policy and legal framework which should detail the purposes for which the data collected may be used. This data is already being held by third parties and used for validation of identity documents. Meaning, it could potentially be used for more efficient delivery of services to the people. However, this must be done under principles that protect and promote rights, hence the need to address fairness in data processing. There are also long term issues in the data economy such as access to the internet, and building Kenya's capacity for the new economy that require policy intervention. While large private companies may already be practising data protection and have the capability to adopt new standards once a data protection framework is adopted, this may not be the case for micro, small and medium enterprises (MSMEs) or academic institutions. Interventions are therefore required to ensure that MSMEs build their capacity to promote the highest levels of data protection.

It is therefore recommended that a policy and legal framework for data protection be developed and that it includes an independent authority to oversee fair and just processing of data while promoting the data economy. An ideal data protection framework is one centred on the person. Lack of awareness and consent of the data subject, exclusively automated data processing and opaque data management practices can lead to lack of fairness in data processing. Transparency is therefore identified as a best practice that should be included in the policy and legal framework. This framework would cover how personal data is collected, and promote and protect rights through getting informed consent from the data subject. Further, it would give the data subject the opportunity to view, access and request for rectification of their data. In addition, they would be protected from decisions made purely through automated processes and be notified in case of breach of their data.

This policy brief examines the current state of data protection in Kenya and recommends the development of a consolidated framework to provide for data protection principles. It further proposes the establishment of an independent authority to promote data protection and enforce the law. Accordingly, the government should develop a privacy and data protection policy that also covers digitalisation of public records, and Parliament should urgently enact a data protection law.

GLOSSARY OF TERMS

Personal data	Facts or information that can be used to identify a person
Sensitive personal data	Data that reveals sensitive personal traits such as genetics, biometrics, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health status or sex life/ sexual orientation
Anonymous data	Data that does not allow that a person can be identified
Data processing	Converting of data into information. This includes collecting, recording, rationalizing, storage, alteration, retrieval, use, transmission, dissemination, erasure or destruction of data
Data processor	One who processes data, whether for themselves or on behalf of another
Data controller	One who designs how data will be processed and may sometimes give the data processing job to a data processor such as a mall that decides to hire a security company to install CCTV cameras to capture the traffic in and out of the mall
Data subject	The person that data relates to
Genetic data	Data that uniquely identifies a person based on inherited and acquired traits. Typically involves processing of biological samples for physiological and health information
Biometric data	Personal data used to identify a specific person using human characteristics such as fingerprints, face recognition, DNA, eye parts, voice and body odour

INTRODUCTION

Data is a powerful tool in the development of our society. Its potency comes with many risks, for instance profiles from personal data can be used to exploit people and lead to further discrimination and marginalisation.

Data protection is a relatively new and evolving area of law and policy in particular in the African region where only 17 out of 55 African countries have data protection laws. It defines how the privacy of individuals is protected whenever their data is collected, used or disseminated. Privacy is the state of being apart from other people. Ideally, a person should be able to limit how aspects of their personality are seen on the public or private sphere. Protecting privacy is grounded on the notion of human dignity and autonomy on one hand and social order on the other.

The use of digital technologies in data processing has increased both the volume and scale of data processing. Activities that previously required hours in travel and physical presence are increasingly being done online.[1] For example, filing of taxes, application for passports, driver's licenses, trade permits and professional licenses are now done exclusively online. Payment of goods and services using virtual money has also increased as have social connections with friends and relations through mobile phones.[2]

The world over, policy makers are deliberating on the effects of digitalisation on society, with a view to responding to issues such as data privacy, data residency, data and democracy, and autonomy of users in data-driven decisions. Digitalised services create databases using personal information. Such information can be used to study subjects and predict future behaviour. For example, the analysis of a person's mobile money transactions can give comprehensive ideas of the person's product preferences and geographical areas where they have interest. With the analysis, marketers can predict products that the person would likely purchase.

The same data can also be used for non commercial purposes such as efficient government service delivery, behaviour change and political manipulation. During the 2013 and 2017 Kenyan general elections, it was reported that data collected from mobile money agent transactions records was used to register people into political parties without their knowledge. In 2017, data from government databases was used to mobilise people in certain areas to register as voters and it is highly probable that the same data was also used to profile voters and micro target them.[3]

1 GoK, "ECitizen | A Portal That Offers Access to Information and Services Provided by the Kenyan Government," eCitizen portal, accessed April 5, 2018, https://www.ecitizen.go.ke/ecitizen-services.html

2 GSMA, "GSMA Mobile Economy 2018," 2017, https://www.gsma.com/mobileeconomy/.

3 Privacy International. Further questions on Cambridge Analytica's involvement in the 2017 Kenyan Elections and Privacy International's investigations. March 2018, https://medium.com/@privacyint/further-questions-on-cambridge-analyticas-involvement-in-the-2017-kenyan-elections-and-privacy-15e54d0e4d7b

Examples of use of personal data

POLICE CASE NO. 121 /
Date to court: / /201
COURT file NO. /1

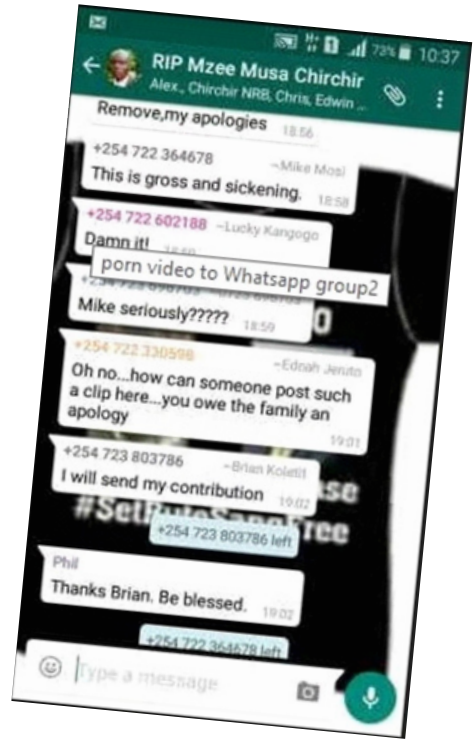
O.B. NO: 29/ /04 /2015

Christian Names in full or Name	Surname or Father's Name	Passport/ID Number	Sex	Nationality or tribe	Apparent Age	ADDRESS(include district and Location where Applicable)
GEOFFREY	ANDARE	26071285	M	KENYAN	ADULT	LUO

CHARGE IMPROPER USE OF LICENSED TELECOMMUNICATION SYSTEMS CONTRARY TO SECTION 29(b) OF THE KENYA INFORMATION AND COMMUNICATION ACT CAP. 411A LAWS OF KENYA.

PARTICULARS OF OFFENCE (See Second Schedule of C.P.C.) **COUNT 1**

GEOFFREY ANDARE – ALIAS **andre Jeffrey** On 23rd March, 2015 at unknown place within the Republic Of Kenya, using facebook account andre Jeffrey posted grossly offensive electronic mail *"you don't have to sleep with the young vulnerable girls to award them opportunities to go to school, that is so wrong! Shame on you"* knowing it to be false and intended to cause annoyance to Titus kuria.



> *Based on the country's national values and principles that envisage a plural society where every individual is facilitated to achieve their destiny, the law should provide the highest protection for the person.*

Going forward, more data will be collected and processed by various actors such as the state and private service providers. In the US for instance, automated data processing is being tested and in some cases used in making decisions such as sentencing in criminal cases, medical diagnosis and treatment, management of transport and delivery of utilities such as water and electricity.

This policy brief reviews data protection in Kenya as provided for in various statutes and practices. It also considers past efforts for a general data protection regime, pointing out how these could be improved. Considering that issues in data have evolved beyond data privacy and user autonomy, to re-purposing of data and political data, the brief further explores policy issues on data protection.

In addition, it is from this background that recommendations for a comprehensive data protection framework for Kenya are made. These include principles for data protection, and creation of an independent regulatory authority as is the case of countries such as Ghana. This will ensure real progress for the society as a whole, as the principles to guide how to use data while strictly protecting personal privacy will be defined.

Accordingly, Kenya's data protection law should be forward looking. Based on the country's national values and principles that envisage a plural society where every individual is facilitated to achieve their destiny, the law should provide the highest protection for the person. It should also create a framework that gives a high standard for privacy in order to make the country attractive for the data economy. The framework should include principles for data protection, relationships between the various actors as well as enforcement mechanisms.

Data protection in Kenya

Protections for personal data are found in various laws, professional codes and court judgments.

This section provides a brief explanation of how data is protected in the current laws, and contrasts that with data collection practices by the government and private actors.

Laws such as the Official Secrets Act which classifies government information, provide some protection to personal data. Other examples are the protection through anonymisation of minors, patients and witness identities under Children's Act, HIV and AIDS Prevention and Control Act, and the Witness Protection Act.

Personal financial information is protected through confidentiality requirements under the Banking Act, Credit Reference Bureau Regulations and Capital Markets Act. Laws that require publication of data such as the Access to Information Act and the Public Archives and Documentation Service Act also have inbuilt mechanisms for protection of personal information. These include anonymised publication of data, redaction of sensitive personal information and obscuring of the person in question. Under the Kenya Information and Communications Act, it is an offence to intercept messages. The Private Security Regulation Act protects data collected during entry into buildings from being used for other purposes. The ICT Regulations under the Elections Act provide for the protection of biometric data collected during elections.

Personal data may also be protected by binding professional codes of ethics. For example, advocate client privilege and doctor patient confidentiality prevents sharing of personal data with a third party. Similarly, media codes protect information such as sources, victims and minors details from being published while academic research anonymises sensitive personal data.

Courts have weighed in on different aspects of the right to privacy. Prior to the 2010 Constitution, privacy petitions were grounded in access to information held by the state, the evidentiary value of information collected during illegal search and seizure, evidence in possession of third parties relating to private or privileged communication, and disclosure of HIV/AIDS status.

After the enactment of Kenya's 2010 Constitution, privacy has been considered alongside other rights in petitions related to property rights. It has been held that petitioners claiming rights protection must show how they are affected by the action alleged to be a breach of privacy.[1] In one case, the court declined to order a DNA test in consideration of the respondent's privacy rights where the petitioner had not proven their claim.[2]

Issues of dissemination of personal pictures[3] and minors' photographs[4] have also been considered. Others include information privacy cases such as commercial appropriation of the likeness of a person[5] and potential privacy breaches with thin SIM card technology.[6]

In April 2018, the High Court found that installation of a Device Management System (DMS) to access information on the International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), Mobile Station Integrated Subscriber Directory number (MSISDN) and Call Data Records (CDRs) of subscribers with the objective of weeding out counterfeit phones would limit the right to privacy. It therefore held that such limitation should be done in strict conformity to Article 24 of the Constitution that provides for limitation of fundamental rights and freedoms. This includes rationality, necessity and proportionality.

Kenya attempted to regulate data protection through two bills in 2009[7] and 2012.[8] The 2009 draft was not envisaged to apply to private sector data, while both bills covered only automated processing of data. The 2009 Bill created a data protection commission while the 2012 one proposed to give that role to the existing government ombudsman. Both bills did not adequately address rights of data subjects and issues of consent, data residency and portability and cross border transfer. Neither of the bills was introduced in Parliament.

The penultimate section of this paper discusses what an ideal data protection framework for Kenya should look like, and identifies two key issues for improvement of the bills. These are inclusion of data protection principles, and establishment of an independent data protection authority (DPA).

1 Standard Newspapers Limited & another v Attorney General & 4 others (High Court at Nairobi October 17, 2013).

2 S.W.M v G.M.K (High Court at Nairobi October 5, 2012).

3 Roshanara Ebrahim v Ashleys Kenya Limited & 3 others (High Court at Nairobi December 7, 2016).

4 Charles Muturi Macharia v Standard Group & 4 others (February 2, 2017).

5 Rukia Idris Barri v Mada Hotels Ltd (High Court at Nairobi August 22, 2013).

6 Bernard Murage v Fineserve Africa Limited & 3 others (High Court at Nairobi May 29, 2015).

7 Republic of Kenya, "Data Protection Bill" (2009), https://www.ifex.org/kenya/2011/11/09/kenya_article19_data_protection_bill_final.pdf.

8 Republic of Kenya, "Data Protection Bill" (2012), http://icta.go.ke/data-protection-bill-2012/.

Data processing by government

During the presidential election petition in August 2017, the Supreme court was informed that election data in custody of a French contractor could not be accessed due to time zone differences.

The privacy of personal data is limited through laws and practice. The Prevention of Terrorism and National Intelligence Service Acts limit the right of privacy for persons suspected of terrorism and offences under national security respectively. Collection of personal data is also sanctioned under the Private Security Regulation Act that ratified the common practice of producing an identity card for registration of personal data before accessing public and private buildings. Mandatory SIM card registration requires telecommunication operators to maintain a register of all subscribers on their network. This links automatically collected data from mobile phones on their network to identifiable persons. A prerequisite for use of mobile money services is registration of personal data such as phone number and national identity card number for almost every transaction. The 2017 Civil Aviation (Remote Piloted Aircraft Systems) Regulations[1] which allow the use of drones subject to thorough scrutiny from the Ministry of Defence and the Kenya Civil Aviation Authority create the potential for indiscriminate collection of personal data.

The government has ICT based surveillance systems that collect a wide range of data. These include internet traffic monitoring equipment (NEWS), National Surveillance Communication Command and Control System (NSCCCS) that has street based ccTV surveillance, the Device Monitoring System (DMS) , biometric immigration services and among others.

In 2015, President Kenyatta launched the Integrated Population Registration System (IPRS) which centralises identity data from state databases. This consists of birth, death, marriage, elections, tax, drivers, education, National Social Security Fund (NSSF) register, National Hospital Insurance Fund (NHIF) register and, the Kenya National Bureau of Statistics (KNBS). The objective of the system is to uniquely identify each and every person in Kenya using one identifier from birth to death. The system also serves to validate and verify identity documents by giving access to third parties such as banks and mobile network operators who are required to register and authenticate their customers.

1 The Civil Aviation Regulations. http://kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2017/259-CivilAviation_RemotePilotedAircraftSystems_Regulations_2017.pdf

The now defunct Commission for Implementation of the Constitution (CIC) had drafted a Registration and Identification of Persons Bill that made provision for registration of Kenyan citizens at birth. The Bill aimed to cure the problems associated with lack of official identification among a section of Kenyan citizens. A version of the Bill was introduced in the last Parliament but not concluded.[2] The IPRS project is therefore being undertaken in the absence of a policy and legal framework that defines the objectives, actors and policy balancing between provision of security by the government and protection of privacy and other rights of citizens.

Some of the projects implemented under the IPRS framework include the e-citizen portal, transport integrated management system (TIMS), and the National Education Management Information System (NEMIS). The systems are developed by private contractors who collect, process and keep data. In the case of e-citizen, ongoing litigation reveals that the system was operated and managed by a private company,[3] creating concerns about retention of personal data by the contractors. During the presidential election petition in August 2017, the Supreme court was informed that election data in custody of a French contractor could not be accessed due to time zone differences.[4]

Counties such as Nairobi, Mombasa, Kiambu and Murang'a have developed automated revenue collection systems through which residents make payments such as licence fees, land rates and parking fees. Many of the systems incorporate mobile money for ease of payment and collect personal data such as ID card details, phone number and residential address. Some of the information is retained by service providers contracted to run or maintain the systems.

2 Registration and Identification of Persons Bill" (2014), parliament.go.ke/the-senate/house-business/senate-bills/item/988-the-registration-and-identification-of-persons-bill-2014

3 Franklin Sunday, Treasury: Millions Paid for Ecitizen Services Ended in Private Accounts,"The Standard, January 16, 2018, https://www.standardmedia.co.ke/business/article/2001266099/unmasking-the-legal-fight-behind-ecitizen-deal-worth-billions

4 Walter Menya and John Ngirachu. Raila Odinga's lawyers and IEBC row over server access. AUGUST 29 2017. HTTPS://WWW.NATION.CO.KE/NEWS/NASA-IEBC-SERVERS-ACCESS-DENIED/1056-4074952-M6Y5VR/INDEX.HTML

Data processing by private entities

Autonomous state agencies and private actors have also been adopting biometric identification systems. For example, the Kenya Commercial Bank (KCB) in December 2017[1] invited bids from technical experts for deployment of biometric authentication technology for their customers. Equity Bank[2] and the Standard Chartered Bank[3] Kenya have already implemented fingerprint authentication.

Safaricom's Jitambulishe[4] is a voice biometric service used for authentication. The University of Nairobi[5] records student registration and attendance via biometrics. The Law Society of Kenya has also procured a biometric member's service system. Many private businesses use biometrics to monitor entry into their premises and manage human resources.

In cases such as the Law Society of Kenya[6] and the University of Nairobi, biometric registration is a mandatory prerequisite to access services from the entities. The systems are implemented and maintained by private service providers who gain access to customers' personal data in the course of installing and maintaining the systems. Most of the customers do not understand the purposes for which their data is collected or whether it is stored securely. Similarly, mobile loan apps such as Tala[7] collect extensive data on customers' financial habits to analyse it for credit scoring. Customers do not seem aware that the data is shared with other credit scorers and some of the collection of data occurs ubiquitously.

Kenya is among Africa's most connected countries with a mobile penetration rate of 88%.[8] Mobile Network Operators (MNOs) collect varied data from subscribers including location and call history. This data is identifiable as SIM card regulations require mandatory registration of SIM cards before they are activated. MNOs also collect data on mobile money transactions. Where customers use an agent to access mobile money services, the agent collects data such as identification document details and transaction amount.

In addition those who use online services such as Uber, Google, Facebook have identifiable data about them collected. This may include their internet protocol (IP) Address, the unique number through which a device accesses the internet, social networks, financial and local information.

1 KCB, "Implementation of Biometric Authentication," December 2017, https://ke.kcbgroup.com/about/tenders/item/35

2 George Ngigi, Equity Bank Bets on Biometrics to Curb Fraud, Business Daily, November 24, 2014. https://www.businessdailyafrica.com/markets/Equity-bets-on-biometric-IDs-to-curb-fraud/539552-2533664-yfmato/index.html

3 Victor Juma, StanChart Launches Fingerprint Banking Technology in Kenya. Business Daily. December 7, 2016, https://www.businessdailyafrica.com/corporate/StanChart-launches-finger-print-banking-technology-in-Kenya/539550-3478696-131ss2j/index.html

4 Safaricom Ltd. Safaricom Introduces Voice Biometrics to Enhance Customer Experience. December 11, 2017. https://www.safaricom.co.ke/about/media-center/publications/press-release/release/408

5 UoN. Students to Start Using Biometric Cards. April 11, 2018. http://www.uonbi.ac.ke/content/students-start-using-biometric-cards

6 LSK, "Upgrade of LSK Systems and Processes," 2017, http://lsk.or.ke/Downloads/Upgrade%20of%20LSK%20Systems%20and%20Processes_1.pdf

7 https://tala.co/

8 CA, "Kenya's Mobile Penetration Hits 88 per Cent," 2016, http://www.ca.go.ke/index.php/what-we-do/94-news/366-kenya-s-mobile-penetration-hits-88-per-cent

Risks

Without a general data protection framework, it is up to entities that collect personal data to employ internal voluntary strategies such as ISO 27000 Standards on Information Management Systems to protect this data. This creates uncertainly for users, risks fragmentation on application of safeguards and exposes data to breach. And this comes with risks such as identity theft, misuse of personal information, unauthorised distribution and sale of data, financial loss and erosion of privacy.[1]

Further, data may be aggregated and used for purposes other than what it was collected for. In Kenya, mobile phone customers have for example complained about receiving direct advertising in services they did not subscribe to. In some cases, these are premium charge services that have a cost implication. Apart from commercial purposes, data is also a means of conducting surveillance. During the 2017 election period, a Supreme Court judge protested when his mobile phone call logs were shared online.[2] An investigation by Privacy International had linked use of phone data to extra-judicial killings. Beyond individual harm, personal data collections increase the risk of injury to groups. For example, automated decision making can lead to discrimination and marginalisation of groups, through denying or determining access to services based on characteristics that may exacerbate discrimination they already face in society. Other examples include use of personal data to profile voters and spread misinformation, and this has had polarising effects on societies especially at election times.

1 CIPIT, "Biometrics in Kenya", 2018 http://blog.cipit.org/wp-content/uploads/2017/12/Biometrics_defined.png

2 Kamau Muthoni, "Justice Lenaola Protests to Safaricom over Call Logs," The Standard, accessed April 8, 2018, https://www.standardmedia.co.ke/article/2001255316/justice-lenaola-protests-to-safaricom-over-call-logs

Data protection in other jurisdictions

> In the case of Kenya, this right may be useful in the case of records of minors in databases such as the education registry NEMIS. A question for debate would be how long children's records under NEMIS should be kept and to what extent they influence decisions about the children now and in the future.

In the spectrum of data protection, the knob moves from giving individuals as much autonomy as possible over their data on one end, to non-acknowledgement of information privacy on the other.

The European Union (EU) has the highest protection for personal data, requiring accountability from processing personal data of individuals located in the EU. These individuals are entitled to not only consent and fair notice, the right to be forgotten and to object to their data being used for marketing purposes, but also to the right to transfer their data, among other rights. Consent has been defined as a freely given and specific indication by the data subject of agreement to their personal data being processed. Where the purpose for which data was initially collected changes, data subjects need to be informed and consent afresh. Under the General Data Protection Regulations (GDPR), it is not necessary for public bodies in the course of their duties to seek consent of the data subject. Compliance with the law is conducted by independent authorities that are empowered to investigate and sanction public and private actors' misuse of data.

China's cybersecurity law creates data protection obligations on network operators and restricts exportation of personal data.

Closer home, the *African Union Convention on Cyber Security and Personal Data Protection* calls for each state party to establish a legal framework for protection of data and punishment for violation of privacy principles.[1] It envisions protection for genetic information and health research; information on offences, convictions or security measures; national identification numbers; biometric data; and personal

1 AUC. African Union Convention on Cyber Security and Personal Data Protection. (2014),https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

data in public interest in historical, statistical or scientific purposes. Subsequently, close to 20 African countries have enacted data protection legislation. The countries include South Africa[2] and Ghana,[3] both of which adopt the principles of data protection and have an independent oversight authority.

Globally, emerging issues on data privacy include the right to be forgotten and encryption as a part of the right to privacy. Both these issues have been brought about by digitalisation that has eased data processing. The right to be forgotten is the right to have personal data deleted from electronic records. It has taken different forms, such as removal of one's records from search engine results and removal of criminal records after rehabilitation of an offender. In the case of Kenya, this right may be useful in the case of records of minors in databases such as the education registry NEMIS. A question for debate would be how long children's records under NEMIS should be kept and to what extent they influence decisions about the children now and in the future.

Encryption is an enabler of digital rights such as freedom of expression as well as privacy. However, government agencies, in particular law enforcement agencies, continue to argue that it inhibits their capacity to fight high crimes and terrorism as encryption hampers surveillance. The United Nations Special Rapporteurs on Freedom of Opinion and Special Rapporteur on Expression and Privacy caution against governments restricting encryption.

2 See http://www.justice.gov.za/legislation/acts/2013-004.pdf

3 See https://www.dataprotection.org.gh/

Policy concerns

The fourth industrial revolution is often characterised as the convergence of the physical, digital and biological spheres. Previous industrial revolutions created new forms of property ownership such as trade secrets, copyright, geographical indications, patent, trademarks and brand equity. In the digital age, data is also emerging as a new form of property with contestation as to its ownership. One school of thought views the data subject as the owner of the data while another views the data as trade property of the data processor or controller. Whichever doctrine is applied, advances in data processing have rekindled debate on the value of the data subject or person.

Policy concerns can be considered from three prongs: economic issues, fairness in data processing and political data.

Economic issues

With the digitalisation that is taking place in Kenya, the country has a growing data economy. Activities in the emerging economy have mostly focussed on data production as is the case with the government digital identification programme and collection that is undertaken by private parties such as MNOs, professional and education institutions among others. It is anticipated that the next step will entail more processing activities such as analysing and applying the data in decision making. Economic issues arising from the increasing data production include defining value of data, government readiness for the data economy, digital divides and equity for micro, small and medium enterprises (MSMEs).

A foundational issue in crafting a modern data protection law is that of property of the data. When one uses a mobile phone for instance, at a minimum, they generate data about their device, location and those they connect with. This data has economic value because when collected over time, it creates a profile of the person, their habits and networks. Such a profile can be used to target services to the person creating an increasing demand for data. Examples of targeted services include marketing information, emergency response, and political propaganda. When data is a market commodity produced by the data subject, the question of an economic exchange between the data subject and processor arises. It may be argued that in exchange, data subjects enjoy conveniences such as easier

access to credit and insurance and personalization of products and advertisements. A people-centric data economy such as the European Union has taken a paradigm shift, by expanding the data subject's autonomy to control their data. Future looking data protection regimes may also have to accommodate other models of data ownership such as cooperatives where data subjects are also data controllers.

The government of Kenya identifies ICT as a pillar for economic prosperity in its Vision 2030 as well as ICT Policy. In its second term, President Kenyatta's administration aspires to leverage on distributed ledgers and internet of things to create a new digital economy. Data impacts a spectrum of fields from city planning and design, law enforcement, warfare and security, education and research, health, marketing and consumption, journalism, actuarial science, the employee rating in employment, credit rating, identity verification and so forth. The data economy will likely benefit from sharing of data held in different databases. For example, Kenya lacks an official addressing system, but private services such as MNOs and Google have most of the data required for such a system. A partnership with the national government would therefore create a primary digital infrastructure. Once the system is in place, data on use of roads would be useful in county government functions such as planning transport routes and emergency service delivery.

Data creates new economic activities such as digital advertising, business process outsourcing, data mining, brokerage and analytics. Young people are already engaging in small data processing jobs. In the 2017 general election, the opposition political party, the Orange Democratic Movement (ODM), used a locally developed mobile application for party recruitment. [1]There is therefore potential for meaningful work for small and medium enterprises if the digitalisation policy includes mechanisms for an equitable economy. Examples of such mechanisms are access to large databases by researchers and small enterprises, and procurement of services from MSMEs. To get more MSMEs in the data economy would require a balancing act between access to big data and protection of privacy. This can be achieved through having a dedicated authority that would facilitate capacity building among MSMEs and promote innovative means of protecting data in their custody. Other mechanisms that could promote MSMEs are graduated sanctions for data violations[2].

As the debate on digitalisation continues, there are still many places in Kenya that do not have access to the internet. In 2016, and prior to Kenya's 2017 general election, the Communications Authority of Kenya released an access gaps study[3] that provided the context for about 11,000 polling stations that had no access to the internet. These are predominantly in rural and underserved areas. Notably, even where there is access, there are many who are not literate and require assistance to access digital services. In current government digitalisation projects, it has become mandatory to access services such as driver's licences, motor vehicle registration, passport application and land registration online. These realities in the digital divide exposes data subjects to higher risk of theft of personal data as well as inaccuracies that may result in delay or denial of services. There is therefore need for concerted effort to sensitize people as they digitalise. Good practices have been noted from consumer education by MNOs and banks for example the PIN yako ni siri yako slogan where customers are reminded that the PIN which they use to access their personal data is their personal secret.

1 James Mbaka, "ODM Targets 8m Members, Has Listed 4m," The Star, Kenya, March 3, 2017, http://www.the-star.co.ke/news/2017/03/03/video-odm-targets-8m-members-has-listed-4m_c1517283 .

2 Tunisia national authority for the protection of personal data. Article 211 discussed in Access Now, "Lessons from the EU General Data Protection Reglation" (AccessNow, January 2018), https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf.

3 Intelecon, "ICT Access Gaps Final Study" (Communications Authority of Kenya, March 11, 2016), http://ca.go.ke/images/downloads/RESEARCH/ICT%20Access%20Gaps%20Report-April%202016%20.pdf.

Fairness in data processing

Data processing is still in its early stages particularly in African countries which only begun digitalisation about two decades ago. As technology advances, there is a rush to acquire and accumulate huge datasets for future processing. The data economy however commodifies the person by making them merely a source of data for production of the data subject's profile. Some issues here include awareness and consent, automated data processing, opaque data management practices and sensitive personal data.

Before such collection takes place, the data subject needs not only to know that data about them is being collected but also consent to this data being collected. In order to give informed consent, the data subject needs to know the purpose for which the data is being collected. They also need to have access to the data about them that has been collected so that they can amend or delete it as necessary. In addition, data subjects should not have their data retained for longer than necessary.

Automated data collection occurs without active input of the data subject. In the example of using a mobile phone, one only needs to switch on the phone for data such as location and phone number to be automatically collected by mobile network operators (MNOs). The same happens when browsing a website. Data about one's machine and location is automatically collected by any number of collectors from the operating system provider, to the browser company and application service provider.

Technology allows for automated decision making from collected data. Take the example of mobile money loan application apps. The apps calculate loan amounts based on data collected from the subscribers financial transactions without human intervention. Technology may not always process data fairly and data subjects should be shielded from decisions that are made solely on automation. For example, credit rating or employment appraisal algorithms may arrive at negative decisions. In such cases the data subject may miss out on opportunities yet no one will be aware of the logic behind the automated decision.

The cornerstone of fairness in data processing is transparency and accountability on the part of the data processor or controller. This requires letting the data subject know about data collection and the data subject's rights with regards to that data. One of the best practices in data processing is notifying the data subject in case of a breach of their personal data.

Above protecting data subjects rights, some regimes also prohibit trade in certain classes of data. For example, France has special procedures for access to health data and does not allow trade in it.[1] And following use of social media data for political purposes in Britain, United States, Kenya and other countries, policy makers are deliberating restrictions to trade in data for political purposes.

1 DLA Piper, "France: New Rules for Processing Patient Health Data," JD Supra, September 7, 2016, http://www.jdsupra.com/legalnews/france-new-rules-for-processing-patient-38984/.

Political data

Political data is particularly sensitive. The last elections in Britain, United States of America and Kenya reveal use of personal data to invasively profile voters and manipulatively persuade or dissuade them from voting in a certain way. While opinion is divided on the effect of manipulation campaigns, it is clear that this kind of propaganda has resulted in polarisation of societies.

Ghana's Data Protection Act binds the state and perceives state departments that process personal data as data controllers under the law. Each state data controller is required to appoint a data supervisor [1]. The General Data Protection Regulations (GDPR) has given special protection to political data. It requires special safeguards where personal data is processed by political parties. Some of the safeguards that have been put include, prohibition from repurposing personal data made public on the internet for the purposes of political communication; requirement for informed consent before aggregation of personal data of voters for profiling; and guidelines for use of analytic companies in political campaigns. [2]

In Kenya's case, the government IPRS databases contain personal data collected for purposes of identification and other government service delivery. This data should not be profiled for political purposes. Instead, the government should state the purposes for which data in its custody is being used and also update citizens. And where practicable, seek their consent, when the data is repurposed. Given that political parties form the government, there should be an independent data authority to oversee data protection.

1 s. 91, Ghana Data Protection Act

2 European Data Protection Supervisor, "EDPS Opinion on Online Manipulation and Personal Data," March 19, 2018.

What should Kenya's data protection framework address?

With the country's digital advancement, there has been convergence of services resulting in an increase in data processing in many public and private entities. This makes a case for a general data protection law that would provide for lawful data processing.

The enactment of a data law would therefore achieve two objectives:
1. Kenyans would be protected from harms that may accrue from overly broad, risky or malevolent data handling; and
2. Reputable data protection framework that would open up the data economy to more data related work while ensuring trust.

Fairness and lawfulness	Personal data should be processed for a lawful purpose, and those whose data is being collected should be notified as to why their data is being collected. Further, how it will be stored and used.
Stated purpose	Those who collect data should use it for the stated purpose and data should not be further processed in a manner incompatible with the purpose for which it was collected.
Adequacy	Those who collect data should only collect what is adequate and the minimum needed for the stated purpose.
Accuracy	Personal data should be accurate. Data subjects have a right to have their data updated, corrected and erased.
Retention	Personal data should not be kept for longer than necessary.
Rights of data subjects	These include right of access, damage or distress, prevention of direct marketing, automated decision making, correction of inaccurate personal data.
Security of data	Personal data shall be stored and processed in a secure manner to prevent its misuse.
Cross border transfer	Personal data should not be exported to countries that do have adequate data protection laws.

Enforcement and remedies

Most data protection laws are enforced through a data protection authority. Authorities have both pre-emptive mechanisms such as requirement of registration and assessment of data processors, and reactive powers including enforcement notices and administrative fines. Criminal law may also be used to protect privacy where cybercrimes such as interception of private messages exist.

The United Kingdom[1] and Ghana, for example have requisite registration for data controllers and processors. They are also required to notify the data protection authority in case of violation of privacy of data in their custody.

In the event of a data privacy violation, the data processor may be suspended or stopped from further data processing or penalised. Data subjects may be compensated for loss accruing from the violation. In many jurisdictions, the subjects may also sue in court for judicial remedies. Issues that are considered in designing sanctions include damage caused, economic value of data which is measured by business turnover, other regulation mechanisms and available criminal sanctions.

In Ghana, the data protection commission may on its own motion or in response to complaints issue an enforcement notice to a data controller who is in contravention of the data protection principles. The notice may specify steps to be taken or the manner of processing. It may also require a controller to "rectify, block, erase or destroy other data held by the data controller and which contains an expression of opinion, which appears to the Commission to be based on the inaccurate data". [2]Where a controller fails to comply with an enforcement notice, they may be fined a maximum of one hundred and fifty penalty units or to a term of imprisonment of not more than one year or to both.[3]

Monetary penalties for violations of data privacy are increasingly being adopted. The GDPR sets the maximum fine that can be imposed for serious infringements at €20 million or four percent of an undertaking worldwide turnover for the preceding financial year. [4]Tunisia is considering a graduated approach where first time[5] breaches of data, particularly among small processors receive less severe sanctions compared to repeat offenders .

1 See registration categories at https://ico.org.uk/for-organisations/register/

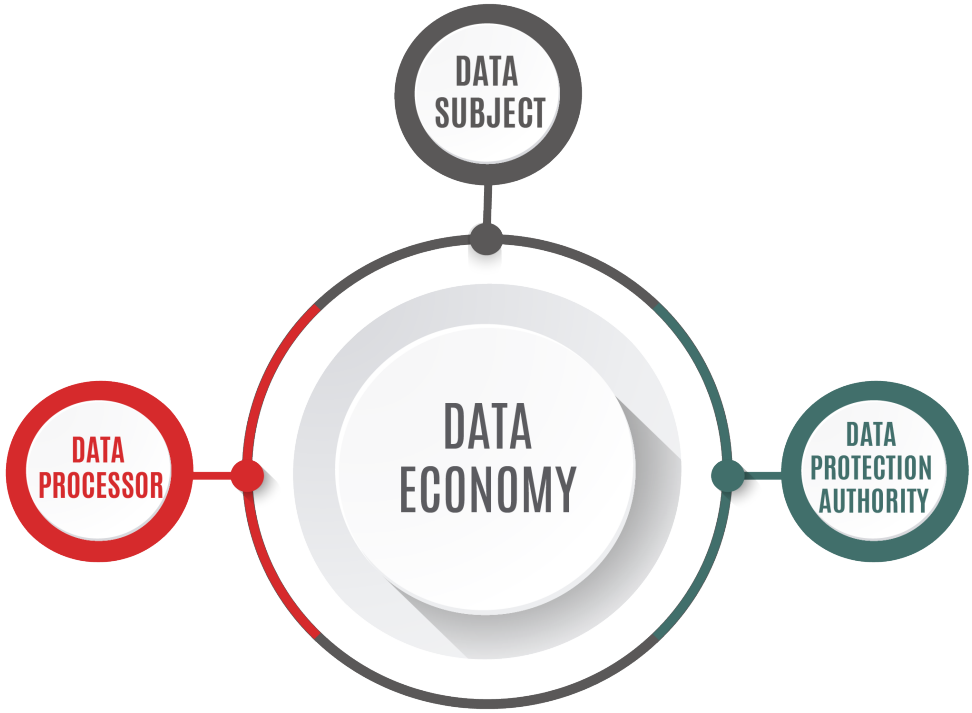
2 s. 75, Ghana Data Protection Act, 2012

3 s. 80, Ghana Data Protection Act, 2012

4 Rec.150; Art.83(5)-(6) GDPR

5 See Tunisia national authority for the protection of personal data. Article 211 discussed in Access Now, "Lessons from the EU General Data Protection Regulation."

Relationships in data protection



In the data economy, key actors include: the data subject who provides the data; the data processor who analyses that data, and the independent authority who regulates the economy.

Data Subject	Data Processor	Data Protection Authority
Should know: • when data about them is being collected • why data about them is being collected • that data about them is being retained and for how long. • when this data is being shared and with whom • when data about them is breached •whether data about them has been collected by data processors including third parties. **Should consent:** • before data about them is collected • before data about them is retained • before data about them is used for other purposes • Should be able to access data about them • Should be able to request rectification of data about them • Should have an option to object to data processing decisions such as automated decision making • Should be able to erase their data when they leave a service Should be able to carry their data across services.	• Should practice transparency in relationship with data subject and data authority **Always promote rights of data subject by:** • Letting data subjects know the purpose for data collection in the simplest terms • Collecting only the necessary and minimal data • Correcting inaccurate data • Deleting obsolete data • Assure data integrity and security, promote privacy by design and by default • Have a clear and easily accessible complaint mechanism and expeditiously resolve issues raised by data subjects.	•Promote and protect data subject rights •Educate the public on the data economy and data subjects rights •Advise private and public entities on emerging issues in data protection •Promote facilitative environment for data processing business including SMEs •Promote adoption of data protection standards among data controllers and processors •Enforce the data protection law, be able to investigate and have the ability to issue sanctions •Dispute resolution

Recommendations

•To achieve a people centred digital economy, Parliament of Kenya should as a matter of priority, urgently enact a data protection law that engenders the data protection principles to afford the highest protection for privacy and other rights for Kenyans.

•Having noted that government of Kenya, through its departments, agencies and public bodies is also a data processor and controller, the framework should also provide for independent oversight of data protection through a data protection authority, that also covers data processing activities conducted by both private and public entities.

•There is an existing data economy in Kenya that includes big players, research institutions as well as MSMEs. Development of the data protection legislation should involve all stakeholders.

•There is no policy framework for the IPRS government identification project. This should be cured through the immediate provision of information on the objectives of the project and purposes for which collected data will be used. In addition, a registration and identification of persons bill should be introduced in Parliament and subjected to public participation.

•There are many private entities which process large amounts of personal data. Some may be able to ratify the processing of such data and make it lawful through acquiring consent of the data subjects, and educating them on the purposes for such collection. A mechanism to audit personal data in the custody of private entities should be developed. This would help assess whether such data is required lawfully and how long it should be kept.

ANNEX: Example of recent goverment data processing systems

Transport Information Management System -TIMS

NTSA is set to issue smart drivers licenses according to the NTSA Strategic Plan 2014 – 2018. The Authority set up the Transport Integrated Management Systems (TIMS) with the following modules:

I. Motor Vehicle Registration

II. Driver Testing and Licensing

III.RSL/PSV Management

IV.Motor Vehicle Inspection and Testing

V. Enforcement Management

VI.Citizen Self Service Portal

VII.TIMS Web Interface

VIII.Reporting and BI

TIMS is being implemented in several phases.

Phase 1 of the project involved drivers' licenses being renewed online, while Phase 2 involved getting all information on vehicles and drivers. Phase 3 which is ongoing involves issuing of smart drivers' license while Phase 4 will be connecting the smart driver's license to a digital financial wallet. The second module which is on Driver Testing and Licensing started out with online renewal of Drivers' Licenses. The new generation licenses that the Authority intends to roll out soon will collect data that will be stored in TIMS.

This data will be available for use by interested third parties like insurance firms who may use it to calculate insurance premiums or a potential employer who wants to hire.

National Education Management Information System -NEMIS and Unique Personal Identifiers for children
NEMIS "single source of truth"

The government has introduced a six- character Unique Personal Identifier (UPI). This UPI will be linked to an electronic database with the educational records of all individuals from primary school up to university level. The UPI will also be used to curb the theft of public funds by eliminating 'ghost' teachers and inflated student enrolment figures. This UPI program has been introduced under the National Education Sector Plan (NESP) Volume Two: Operational Plan 2013 – 2018 that was published in the year 2015.

The Kenya National Education Management Information System (NEMIS) goal is to be a viable system of authentic sector-wide information management based on IT databases that compile, collate and report on relevant information at all levels of the education system. The primary purpose of NEMIS is to support the implementation of NESP and centralise all education sector operational activities of the Ministry, Teachers Service Commission and other relevant agencies. This will be done by providing timely and accurate information for strategic planning, policy development and analysis, teacher work force management and operational management.

The former Education Cabinet Secretary Fred Matiang'i described UPI as "the single source of truth for information" as it will consolidate data from all the Ministry of Education institutions. The identifier will take the form 'AAA-BBB' and it will be used at every level of education. It will enable interested parties to track the academic progress and qualifications of all persons, which according to Ministry officials, will effectively deal a blow to cheats who resort to bogus academic papers.

Its implementation is through schools where parents are required to provide their details and those of the child for input to NEMIS. Schools forward collected paper forms to education officers who key in the data into the system. At the moment, there are no mechanisms for parents or children to view or verify the data. Most parents do not clearly know the purpose for data collection other than that it is linked to the examination system. Overall, NEMIS is the single largest database of personal data for Kenya's largest population demographic- youth below the age of 35.

KaribuKICTANet :
We invite you to partner

Follow us on twitter @KICTANet
www.kictanet.or.ke
Email: info@kictanet.or.ke