

Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: 1360-0834 (Print) 1469-8404 (Online) Journal homepage: http://www.tandfonline.com/loi/cict20

Rebooting democracy? Political data mining and biometric voter registration in Africa

Alexander Makulilo

To cite this article: Alexander Makulilo (2017) Rebooting democracy? Political data mining and biometric voter registration in Africa, Information & Communications Technology Law, 26:2, 198-212, DOI: 10.1080/13600834.2017.1321097

To link to this article: http://dx.doi.org/10.1080/13600834.2017.1321097

Published online: 27 Apr 2017.

Submit your article to this journal

Article views: 21

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
http://www.tandfonline.com/action/journalInformation?journalCode=cict20

Download by: [INASP - Tanzania] **Date:** 02 June 2017, At: 02:05

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW, 2017
VOL. 26, NO. 2, 198–212
https://doi.org/10.1080/13600834.2017.1321097

Routledge
Taylor & Francis Group

Check for updates

Rebooting democracy? Political data mining and biometric voter registration in Africa

Alexander Makulilo

Department of Political Science and Public Administration, University of Dar es Salaam, Dar es Salaam, Tanzania

ABSTRACT

The introduction of biometric voter registration and biometric voter identification on election day is a new trend in most African countries. This development in turn has necessitated massive political data mining. Yet, the nexus between elections and technology poses challenges on protection of personal information. This article offers a critical discussion of legal and regulatory frameworks that govern protection of personal information in an election context. Using the international standards for personal data protection and lessons from Kenya and Ghana, it notes that Tanzania does not have a systematic regime for personal data protection. This leaves voters' personal data without adequate protection. Accordingly, the adoption of the biometric technology in the process of registration of voters creates greater potentials for violations of personal data than it was the case with the optical mark recognition technology.

KEYWORDS

Biometric voter registration; voting; democracy; Tanzania; privacy

1. Introduction

The democratisation process in sub-Saharan Africa that occurred in 1990s falls under what is popularly known as the 'third wave of democracy'. It was Samuel Huntington, a political scientist at Harvard University who conceptualised the 'third wave of democracy' in his article published by the *Journal of Democracy* in 1991 and later on expounded it in his 1991 book titled *The Third Wave: Democratisation in the Late Twentieth Century*. The wave of democracy provides an expression of democratisation process as a moment of advancement and retardation. In the modern world, Huntington notes at least three major waves:

> The first 'long' wave of democratization began in the 1820s, with the widening of the suffrage to a large proportion of the male population in the United States, and continued for almost a century until 1926, bringing into being some 29 democracies. In 1922, however, the coming to power of Mussolini in Italy marked the beginning of a first 'reverse wave' that by 1942 had reduced the number of democratic states in the world to 12. The triumph of the Allies in World War II initiated a second wave of democratization that reached its zenith in 1962 with 36 countries governed democratically, only to be followed by a second reverse wave (1960–1975) that brought the number of democracies back down to 30. Between 1974 and

CONTACT Alexander Makulilo makulilo76@udsm.ac.tz
© 2017 Informa UK Limited, trading as Taylor & Francis Group

> 1990, at least 30 countries made transitions to democracy, just about doubling the number of democratic governments in the world.[1]

It is important to note that the 'wave thesis' is essentially based on electoral competition. While electoral competition is not a substitute for democracy, it remains an indicator of democracy today. As such, the third wave (1974–1990) predicated the end of authoritarianism through the ballot box, but that has not yet happened. It is contended that by 2001 five dozen regimes blended liberalisation with repression and signified the durability of authoritarianism during a period that had augured global democracy.[2] In simple terms, the 'third wave of democracy' marked, among other things, the transition from single party authoritarian regime to multi-party democracy. In the latter, the conduct of regular and competitive elections is among its main features. Other important elements of a democratic regime include adherence to rule of law, existence of an independent judiciary, accountability of a government of the day to its electorates through legislative bodies, existence of the bill of rights as well as the presence of free media and freedom of expression.

This article focuses on the use of technology in elections and protection of the right to privacy in Africa. This focus is further narrowed down to one specific stage of electoral cycle, that is, voter identification through the biometric voter registration (BVR). More than any other stages in the electoral cycle, voter identification involves data mining in creating a voter register and database to support voter registration systems. The article therefore offers a critical discussion of legal and regulatory frameworks that govern protection of personal information in an election context. Using the international standards for personal data protection and lessons from Kenya and Ghana, it notes that Tanzania does not have a systematic regime for personal data protection. This leaves voters' personal data without adequate protection. Accordingly, the adoption of the biometric technology in the process of registration of voters creates greater potentials for violations of personal data than it was the case with the Optical Mark Recognition (OMR) technology. In order to accomplish this endeavour, this article is subdivided into nine sections. Section 1 of this work provides an introduction. Section 2 conceptualises the term political data mining. Section 3 revisits the international standards for personal data protection. Section 4 deals with the nexus between elections and technology. Section 5 focuses on the experience of voter registration in Ghana and Kenya. Sections 6, 7 and 8 provide a discussion on the legal and regulatory frameworks for voter registration and data privacy in Tanzania. Section 9 concludes the article.

2. What is political data mining?

To understand the term political data mining requires in the first place an understanding of the concept data mining. The latter refers to an extensive collection, storage, use and distribution of data based on a particular pattern. This is due to the rise and development of modern technologies which have made it possible for organisations as well as individuals to make data correlations quite easily in achieving certain purposes. Technically, therefore, data mining is the process of finding correlations or patterns among dozens

[1] SP Huntington, 'Democracy's Third Wave' (1991) 2 JD 12.
[2] J Brownlee, *Authoritarianism in an Age of Democratization* (Cambridge University Press, 2007).

of fields in large relational databases.[3] Applied in the field of electoral studies, data mining involves collection of vast amount of personal data about eligible voters. This information can be analysed for various purposes such as determining who will vote for which candidate in an election. In this case, political party's membership information, opinion polls as well as data in the voter register may be extracted for purposes of data mining. It is important to understand that political data mining has implications on an individual's fundamental rights, one of which is the right to protection of one's privacy which is discussed in detail in the subsequent parts of this article.

3. International standards for personal data protection

The international privacy framework offers the standard from which national legislation may be measured against. It constitutes both binding and non-binding data privacy codes. There are two sets of this framework. The first set constitutes human rights norms found in human rights instruments and the second one comprises specific instruments or codes of data protection. Generally, the human right norms of privacy spell out the normative basis of the data protection laws. They are broad statements of privacy protection which have to be implemented by specific privacy codes. The United Nations (UN) has two important instruments namely the Universal Declarations of Human Rights (UDHR) 1948 which states in Article 12 that 'no one shall be subjected to arbitrary interferences with his privacy, family, home or correspondence, or to attacks upon his honour or reputation'. Article 17 of the International Covenant on Civil and political Rights (ICCPR) 1966 reproduces, almost word by word, the content of Article 12 of the UDHR.

The above provisions are similarly provided in almost all regional inter-governmental bodies except the African Union (AU). In Europe, for example, the European Convention on Human Rights 1950 states in Article 8 that

> 8(1). Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

It is interesting to note that specific data protection framework did not develop at the first time at the UN level. The first international privacy code was developed by the Organisation for Economic Co-operation and Development (OECD) in 1980. It is not a binding code. It is in the form of privacy guidelines, hence the OECD Guidelines Governing the Protection of Privacy 1980 (i.e. OECD Privacy Guidelines). The OECD Privacy Guidelines have eight basic data protection principles:

(a) *Collection principle* – that personal data should be collected lawfully and for a specified purpose.
(b) *Use Principle* – that personal data should not be used for purposes that are inconsistent to the original purpose unless there is consent of a data subject.

[3]Anderson Graduate School of Management at UCLA, 'Data Mining', Bill Palace (1996) <http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/index.htm> accessed 3 December 2016.

(c) *Data Quality Principle* – personal data used for a decision affecting individuals should be relevant to the purposes for which they are used and, to the extent necessary for those purposes, should be accurate, complete and up-to-date.
(d) *Individual Participation Principle* – an individual should provide notice to the individual that personal data are being used, and should make readily available to the individual, without charge, a clear and understandable description of the type of data used, its source, how it will be used as well as the legal rights of an individual.
(e) *Openness Principle* – there should be a policy of openness about practices and policies with respect to processing of personal data.
(f) *Security Safeguards Principle* – personal data should be protected by reasonable security safeguards against external and internal risks including unauthorised loss, access, destruction, use, modification or disclosure.
(g) *Accountability Principle* – that data controllers and processors are responsible for compliance.
(h) *Enforcement Principle* – nations should have in place adequate regulatory arrangements, competent bodies and appropriate financial and human resources to ensure that laws enacted pursuant to these Principles are enforced.

The second international code of data privacy is the Council of Europe (CoE) Convention 108 on Protection of Individuals with regard to the Automatic Processing of Personal Data 1981. This is the first binding privacy code. Its significance is that it admits non-CoE member countries to accede. Currently in Africa, Mauritius and Senegal have acceded to the CoE Convention 108 on protection of personal data. Moreover, Morocco, Tunisia, Burkina Faso and Cape Verde have been invited by the CoE to accede to the Convention and its Protocol. Potentially, the CoE Convention is a universal standard. The Convention provides that personal data undergoing automatic processing shall be:

- obtained and processed fairly and lawfully;
- stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are stored;
- accurate and, where necessary, kept up to date;
- preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored;
- properly secured against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Moreover, CoE Convention 108 has a special regime of protection of sensitive personal data as well as transfer of personal data outside its members.

In 1990 the UN developed a specific code for data privacy protection known as the UN Guidelines Concerning Computerised Personal Data Files. It is not a binding code just like the OECD privacy guidelines. The UN Privacy Guidelines has similar principles as the OECD Guidelines. However, the most influential data privacy framework is the European Union (EU) Data Protection Directive 95/46/EC which will be replaced on 25 May 2018 by the EU General Data Protection Regulation 2016. The Directive is binding and through its

restriction of data transfer to third countries which have no adequate level of privacy protection, it has influenced development of data protection law in the rest of the world including Africa and Tanzania in this particular case where privacy law reform is under consideration. The EU Directive has almost identical principles of data protection as the CoE Convention 108.

In Africa, at the continental level the AU has adopted the AU Cyber Security and Data Protection Convention 2014. Part II of this treaty is a data privacy policy. This part incorporates the European data privacy standard as provided in the CoE Convention 108 and EU Directive. The AU Cyber Security Convention is a binding treaty. Although at the time of writing this article, eight African countries had already signed the Convention, it was only Senegal which had ratified it. In West Africa, the ECOWAS Supplementary Act 2010 provides a framework for privacy protection. This is a binding code. Its principles are identical to the AU Cyber Security Convention. The East African Legal Framework for Cyber Laws 2008 contains recommendations for the adoption of data privacy legislation for the East African states. They are neither binding nor elaborate on any principle of data protection. However, they recommend that the East African countries put in place a privacy framework based on the best practices. The Southern African Development Community (SADC) Model Law on Data Protection 2012 offers guiding model for SADC countries to adopt data privacy legislation. The code is not binding.

In summary, it is maintained that the international data protection framework has eight basic data protection principles as demonstrated in the international data privacy instruments. Moreover, an independent supervisory authority is always required in order to effectively implement the privacy principles.

4. The nexus between elections and technology

The rise of modern technology has spurred a variety of uses of technology. In developing countries including Africa, such uses range from civil registries to voter rolls, health records to social transfers, public payrolls to pension payments and beyond.[4] Elections constitute, by far, the largest domain of application of biometric technology in Africa. In at least 20 countries, biometric technology is used for voter identification hence establishments of biometric voter registries. Rarely, biometric technology has been used for authentication during polling. In some few cases, electronic transfer of election results from the polling station to the headquarters of the tallying centre has been made. Kenya is an illustration. The rationale for application of biometric technology in elections is twofold. Firstly, it intends to limit fraud by eliminating chances of multiple registrations in a voter register by one individual. Secondly, it intends to ease authentication process of a voter at polling stations on election day.

In a nutshell, BVR involves the use of biometric technology in capturing personal and demographic data of voters in voter registration process. Through the use of computers, fingerprint scanners and digital cameras, BVR captures the bio-data of applicants. Fingerprints are unique to every individual and it is these unique features and other

[4]A Gelb and J Clark, 'Identification for Development: The Biometrics Revolution' (January 2013), Working Paper 315, Center for Global development, page 2 <https://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf>, accessed 3 November 2016.

details that are normally stored in the computer from which the voters register is produced. Biometric technology incorporates data such as signature, digital photographs and fingerprints and maintains the auditable integrity of voter registration forms that are signed by voters.[5]

The manual method of registering voters did not have an in-built mechanism for detecting multiple registrations and therefore, in most countries there have been instances where some unscrupulous individuals registered more than once. With biometric technology, detection and removal of multiple registrations from the system is easily made possible, hence a more accurate and reliable register. In this case, BVR offers a mechanism for maintaining auditable integrity of voter registration as well as detecting and removing multiple registrations. A biometric method could effectively prevent multiple registrations by cross-checking the digital photographs and fingerprints of the registrants with the fingerprints stored in the national voter database.[6]

Despite the fact that BVR has its own advantages when used for voter registration purpose, it is, however, not a solution to all voter registration problems particularly in developing countries. BVR technology, for example, cannot by itself detect fraudulent registration like the inclusion of foreign nationals or underage voters in the voters' list. It also cannot identify and expunge names of deceased persons from database unless there are further control measures in place. Based on this, BVR therefore should only be seen as a complementary to the necessary tools required for compiling a credible register of voters by election management bodies (EMBs). Furthermore, in order for it to function properly, EMBs staff are supposed to possess essential skills like basic computer skills, with an emphasis on data capture, processing and administration. EMBs staff should also have planning and logistical skills as well as some capacity to repair and maintain equipment. This means that adequate time must be set aside for training of staff involved in BVR.

The use of biometric technology in registration of voters for purposes of elections raises a number of privacy issues. Firstly, such technology has the power to strip an individual of their identities and humanity by reducing them to data profiles to be followed, monitored and watched.[7] Secondly, the collection of biometric data raises two distinct yet interlinked questions: firstly, why it needs to be stored in the first place and secondly, who manages and owns the data and for what purpose it will be used. Recognising the risks of mass data retention, those opposed to biometric databases have argued that there is no need even for their creation to achieve the intended purpose of identification.[8] Thirdly, the retention of data in databases raises questions as to who can access this information, under what circumstances and for what period of time. The management of access is a particularly difficult and challenging area when multiple agencies can access the data for varying purposes and even more so when these agencies are in different countries.[9]

[5]See <http://aceproject.org/electoral-advice/archive/questions/replies/361712092> and <http://www.avantetech.com/products/biometric/biometric-registration/> accessed 29 November 2016.

[6]Coalition of Domestic Election Observers (2012) 'Promoting a Peaceful, Transparent and Credible Biometric Voter Registration Process: Ghana's Election' (2012), page 6 <http://www.codeoghana.org/assets/downloadables/Promoting%20a%20Peaceful,%20Transparent%20and%20Credible%20Biometric%20Voter%20Registration%20Process.pdf> accessed 25 November 2016.

[7]Privacy International, 'Biometric: Friend or Foe of Privacy?' <https://www.privacyinternational.org/sites/default/files/Biometrics_Friend_or_foe.pdf> accessed 20 November 2016.

[8]ibid 14.

[9]ibid 16.

5. BVR in practice: Ghana and Kenya

The use of BVR is relatively new in Africa and Tanzania joins countries such as Nigeria, Kenya, Democratic Republic of Congo, Sierra Leone, Burkina Faso, Zambia, Togo and Uganda in adopting the BVR, supposedly to help produce a register of voters that can be described as legitimate, verifiable and credible. The Electoral Commission (EC) of Ghana introduced national BVR exercise in 2012. Previously, the country used theOMR process to register eligible voters. The register of voters was computerised but the registration process did not include collecting biometric details of the registrants. An eligible voter was required to present him/herself at a registration centre where the OMR scanned form was completed with personal data at specific polling stations. This method had potentials for double or multiple registrations and consequently double or multiple voting as it did not allow for the sharing of voter registration information among polling stations.

The old method of generating a register of voters through OMR proved unsatisfactory, with many people describing it as bloated. There were widespread allegations on bloated registration of voters in the run-up to the general elections in December 2012.[10] In response to irregularities and malpractices associated with old method of voter registration the EC introduced the BVR system. The EC embarked on a national wide BVR exercise in March 2012 to compile a new register of voters in an effort aimed at eliminating the problem of multiple registrations. The BVR exercise in Ghana was conducted from 24 March to 5 May 2012. A series of voter education programmes on various fora and media platforms were conducted by the EC to create public awareness on the BVR exercise prior to its inauguration.

The Coalition of Domestic Elections Observers (CODEO)[11] was of the view that the BVR exercise in Ghana was generally smooth across the country and that the majority of eligible voters had the potential of providing adequate checks against the registration of illegitimate voters. CODEO observation and survey findings further showed that there were several challenges with the implementation of BVR system. They included incidents of equipment breakdown which prevented prospective voters from registering during designated hours; inefficiency in the voter registration system which resulted into long queues, forcing some voters to abandon registration out of frustration; BVR equipment malfunction was the most common of the challenges encountered during the registration period; registration kit malfunction, including login difficulties, screen freezes and printer breakdowns were common across all registration centres. Despite these anomalies CODEO expressed broad satisfaction with the conduct of the BVR exercise towards the 2012 general elections in Ghana.

In Kenya, the Independent Electoral and Boundaries Commission (IEBC) introduced biometric technology in its 2013 elections. Biometric technology aimed at covering two aspects. The first application of technology in the 2013 elections intended to guarantee the integrity of the voter register through the use of a BVR system. The voter registration exercise was conducted over 30 days towards the end of 2012 and was lauded as a success

[10]For more details, see A Bauffour, 'Elections Management and Electoral Politics' in A Bauffour (ed), *Ghana: Governance in the Fourth Republic* (Digital Books Ghana Ltd, 2008).

[11]<http://www.codeoghana.org/assets/downloadables/Final%20Report%20on%20Ghana's%202012%20Presidential%20and%20Parliamentary%20Elections.pdf> accessed 20 November 2016.

with over 14 million voters registered. This voter register was made available at each polling station during the election day in two forms, that is, a biometric Electronic Voter Identification device (Poll Book) and a printed copy. Both of these methods served the same purpose to authenticate the identity of each voter before they voted. The new voter registration system aimed at curbing some of the fraudulent practices of manipulation and vote rigging that were prevalent in the previous manual registration system as specific information such as fingerprints, facial features, name, gender and identification number were biometrically analysed for each registrant.

The second application of technology was to provide an electronic method of transmitting provisional results (votes counted and verified by party agents at polling stations). This was to facilitate rapid announcement of the provisional vote count with results being physically delivered to the national tallying centre for the official, final tally. However, this is one of the most notable technological failures in the Kenyan 2013 elections.

The procurement of the BVR kits during voter registration process in Kenya was blemished with controversy that eroded the confidence in the voters' roll and the commission. A high profiled procurement process of 50 million USD was cancelled occasioning public concern about the IEBC's independence.[12] Procurement problems resulted in a three-month delay and a curtailment of all stages of voter registration. This delay was to have a serious repercussions on elections preparations and ultimately, on the reliability and perceived credibility of the register itself. It was due to this delay that the Elections Act, Cap. 7 R.E 2012 had to be amended to reflect the new timeframes for voter registration, reducing the period for registration from 60 to 30 days, citizen verification from 28 to 14 days and setting the deadline for finalisation of the voter register 14 days before polling, rather than one month before.[13] Given the importance of a credible voter registration process, limited timeframes proved to be challenging. With insufficient BVR kits across the country, the functional throughput was not achieved at the desirable level during registration period.

The voter register that was produced as a result of BVR system was not a subject of controversy until the election day when its weakness led to the use of several different lists. Thereafter, the voter register's reliability was called into question. In conjunction with inconsistent procedures for verifying registration on polling day, this separate list of voters contributed to some of the discrepancies that were later identified in the results. The use of the voter register on the election day did not enable consistently reliable records of registered citizens, nor of how many had voted. Following the failure of poll books (laptops with a full voter register and a fingerprint-reading device), alongside the difficulty in identifying voters in the correct polling stations, a total of four different lists were used: the register in poll books; the lists printed for individual polling stations; the list of people whose biometric data had not been captured, and finally, the entries listed in the 'green books' – the manual records of entries made during voter registration.[14] With regard to voter registration and the Kenyan election of 2013 itself, one thing that stands out is the IEBC's late procurement of both services and equipment

[12]See Election Observation Group (ELOG), 'A Guide to the Kenya 2013 BVR Observation Experience' <https://www.usaid.gov/sites/default/files/documents/1860/THE%20ELOG%20REPORT.pdf> accessed 20 November 2016.
[13]See European Union, 'Election Observation Mission to Kenya: General Elections 2013 Report' <http://eeas.europa.eu/eueom/missions/2013/kenya/pdf/eu-eom-kenya-2013-final-report_en.pdf> accessed 15 November 2016.
[14]ibid 19.

related to the election, and the fact that all technology should have been tested and debugged far in advance before the election. It was the view by many that technical failures that occurred were both foreseeable and preventable and was mostly due to lack of adequate preparations.[15]

On the basis of the experience from both Ghana and Kenya, it can simply be concluded that BVR is indeed a better system for voter registration compared to manual processes of OMR. However, the technology needs to be introduced on time to ensure that it is tested and debugged on a large scale. Moreover training of EMB staff to manage BVR is of critical importance. Proper training would reduce human errors that could be associated with data entry processes.

6. Voter registration in Tanzania: from OMR to biometric technology

The history of the Permanent National Voters' Register (PNVR) in Tanzania dates as far back as 2000 when the Parliament through the Thirteen Constitutional Amendment to the United Republic of Tanzania (URT) Constitution 1977 provided for this registration requirement.[16] Article 5(3)(a) of the Constitution states that Parliament shall enact electoral law to provide for the establishment of a permanent voters register. In 2004 the Parliament through the Electoral Laws (Miscellaneous Amendments) Act 2004 (Act No.13 of 2004) amended the National Elections Act 1985 to establish the PNVR and to provide for other conditions of registration. The PNVR was used for the first time in the 2005 general elections. Prior to this, registration of voters was not permanent. Voters were registered for each specific election. The registration was done manually in special registers and voters were issued with certificate of registration. Following limitations of manual registration for a specific election particularly the issue of identity which resulted into problems of double registration and registration of unqualified voters as well as huge costs of registration a permanent voter register was a solution.

One significant change in the technique of registration after the introduction of the PNVR was the use of OMR technology. OMR is the scanning of paper to detect the presence or absence of a mark in a predetermined position. Information filled by hand is digitally scanned. The PNVR which was based on OMR technology was used for the 2005 and 2010 general elections. The register was updated in 2007/2008 and 2008/2009. It is important to note that the National Electoral Commission (NEC) could not update the register regularly as per the legal requirements due to funding constraints.

The NEC came under serious pressure from various stakeholders, especially political parties, complaining of the failure to update the PNVR since the 2010 general elections and similar problems of identification of voters prior to the introduction of the register. Due to further limitations of OMR, the NEC introduced in 2015 a new technique of registration of voters. This time NEC used biometric technology to register voters hence the genesis of BVR in Tanzania. The BVR is a database of voters in which information related to voter registration is captured through biometric characteristics of each individual. In this case, fingerprints and facial recognition marks of each eligible voter were captured alongside other personal information such as names, dates of birth, physical address

[15] <http://www.aljazeera.com/indepth/opinion/2013/03/2013329135519365308.html> accessed 10 October 2016.
[16] *SheriayaMabadilikoyaKuminaTatukatikaKatibayaNchi, yaMwaka 2000(Na. 3 ya 2000), Kifungu cha 4.*

as well as electronic signature. The NEC announced that all previous voter IDs would thereafter be rendered invalid. The BVR technology would minimise risks of multiple entry and duplication of information of voters registered in different areas and it is more secure in terms of its features compared to the OMR technology. Biometric technology is used to measure and analyse human body characteristics, e.g. fingerprints and facial recognition for either identification or verification purposes. It can therefore easily detect fraud.

It is imperative to note that the voter registration process faced many challenges. The first is the problem of procurement of BVR kits that resulted to a lawsuit, *M/S SafranMorpho Ltd v National Election Commission*.[17] In this case, the appellant challenged the procurement procured by the NEC for acquiring the biometric voter register kits. The *M/S Safran* lost the appeal on technical ground that it had no legal basis to institute the case and also the case was time-barred. It is important to note that the BVR kits were not acquired timely due to financial constraints on the part of the NEC and the government. The other important problem of identification was that the voter registration took place without citizen national identification cards. Although registration of citizen national IDs took place a little while earlier, the NEC insisted that it would not use national IDs for voter registration purposes. In this case, therefore risks of registering unqualified voters were not eliminated. There were also many instances of reported fake voter registration cards and missing information of voters in the PNVR. It was on that basis that the Tanzania Election Monitoring Committee (TEMCO) noted 'No wonder during the updating of the PNVR, the election management body identified 52,062 cases of voters who had registered more than once.'[18] By the end of the registration exercise, the NEC had registered a total number of 23, 161,440 voters for the 2015 general elections.[19]

7. Legal and regulatory frameworks for the BVR

The URT Constitution and the National Elections Act are the main sources of law for the PNVR. The Constitution lays the foundation of the PNVR while the Elections Act provides for the establishment of the PNVR. Article 5(3) of the URT Constitution states that Parliament shall enact electoral law to provide for the followings:

(a) the establishment of a permanent voters' register and prescribing the procedure for its amendment or updating information contained in that register;
(b) specification of places and times for the registration of voters and for voting;
(c) procedure and conditions for enabling a person registered as a voter in one place to vote in another and
(d) specification of the duties and functions of the EC and the procedure for every election shall be conducted under the direction and supervision of the EC.

In compliance with the constitutional requirements, the Parliament amended the Elections Act in 2004 to provide for the PNVR. Section 12(1) of the Elections Act states that there

[17] Appeal Case No. 33 of 2013–14, Public Procurement Appeals Authority, Dar es Salaam (Unreported).
[18] <http://www.temco.udsm.ac.tz/images/stories/TEMCO_Reports/TEMCO_2015_BIOMETRIC_VOTERS_REGISTRATION_REPORT.pdf> accessed 10 December 2016.
[19] <http://www.nec.go.tz/uploads/documents/en/1480489822The%20Report%20of%20the%20National%20Electoral%20Commission%20on%20the%202015%20Elections.pdf> accessed 10 December 2016.

shall be a PNVR for the URT. Under this Act, it is the duty of the Director of Elections to keep, maintain and up-to date the register [s. 12(2)].

As for the type of information which should be captured in the register, the Act states that the register of voters shall consist of names of voters in a polling district [s. 12(3)]. Moreover, the register must show the number of the voter's card issued to him or her, the sex of the voter and address of residence of the voter [s. 12(4)]. The NEC (i.e. Commission) may direct that other particulars be captured in the register [s. 12(4)]. From this general mandate, the Commission also requires a voter to provide his or her date of birth which appears on the voter's card as well as a signature of the voter. During registration, a voter is asked to provide his or her phone number although this does not appear on the voter's card.

The Elections Act provides for two types of voters registers. The first one is called the Provisional Voters' Register (PVR) and the other is thePNVR. In s. 11(A) the Act states that the Commission shall, for the purpose of preparation of the PNVR, establish a PVR. According to this provision, the PVR is used to displaying for inspection by the public; amendments regarding change of residence or any other particulars of the voter; making objections against registration of any voter; inclusion or deletion of a name of a voter in the register and effect any other correction as may be or amendment as required under the Act. Once provisional register is confirmed then such information is used to generate the second type of voter register known as the PNVR. The latter is under the custodian of the Commission [s. 12(5)].

Moreover, the Elections Act makes it an offence for any officer of the Commission or an agent of a candidate to disclose any information as to the name, or number of any voter who has or has not applied for a ballot paper or voted at the station or as to the official mark [s. 93(3)]. Disclosure is only permitted under specific laws.

7.1. National privacy framework

Currently Tanzania has no general data protection legislation. However, protection of privacy is afforded through the URT Constitution and other statutory laws which regulate specific sectors or matters.

The URT Constitution generally guarantees the right to privacy in Article 16. Sub-article one of this provision states, 'every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications.'[20] However, this right to privacy is not absolute. There are limitations in sub-article two. This provision states,

> for the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon without prejudice to the provisions of this Article.

These limitations are provided in Article 30(2) which states:

> It is hereby declared that the provisions contained in this Part of this Constitution which set out the principles of rights, freedom and duties, does not render unlawful any existing law

[20]URT Constitution 1977, Art 16(1).

> or prohibit the enactment of any law or the doing of any lawful act in accordance with such law for the purposes of:-
>
> (a) ensuring that the rights and freedoms of other people or of the interests of the public are not prejudiced by the wrongful exercise of the freedoms and rights of individuals; (b) ensuring the defence, public safety, public peace, public morality, public health, rural and urban development planning, the exploitation and utilisation of minerals or the increase and development of property of any other interests for the purposes of enhancing the public benefit; (c) ensuring the execution of a judgement or order of a court given or made in civil or criminal matter; (d) protecting the reputation, rights and freedoms of others or the privacy of persons involved in any court proceedings, prohibiting the disclosure of confidential information or safeguarding the dignity, authority and independence of the courts; (e) imposing restrictions, supervising and controlling the information, management and activities of private societies and organisations in the country; or (f) enabling any other thing to be done which promotes or preserves the national interest in general.

The High Court of Tanzania (HCT) has laid down guiding principles in interpreting the above Article on limitations of individual's right. The court has always held that a law which seeks to limit or derogate from the basic right of individual on ground of public interest will be saved by Article 30(2) of the Constitution if it satisfies two requirements: if such law makes adequate safeguards against arbitrary decisions and provide effective controls against abuse of those in authority when using the law and the limitation imposed by that law must not be more than necessary to achieve the legitimate object.[21] In *Jackson Ole Nemeteni and 19 Others v the Attorney General*[22] the HCT held that in the absence of a procedure prescribed by law, the administration of a provision of any law which seeks to limit the basic rights of an individual is susceptible to abuse, and cannot therefore be saved under Article 30(2) of the Constitution.[23]

In August 2016 the Law Reform of Tanzania published a public consultation to solicit opinion from the public and stakeholders on a proposed Data Protection Bill. This law will provide the general conditions of processing personal data (i.e. information that can identify a living individual such as name, IDs, biometric information, SIM card, IP address, and DNA). This law is meant to give effect the provision of Article 16 of the URT Constitution on the right to privacy.

The other law that partly regulates privacy is the Electronic and Postal Communications Act 2010 (EPOCA). This Act came into operation in May 2010. EPOCA is a communications sector law. It has very limited provisions on protection of privacy. Like other pieces of legislation in specific fields such as the Banking and Financial Institutions Act 2006; Tanzania Intelligence and Security Service Act, Cap.406 R.E 2002; the Prevention of Terrorism Act, Cap.18 R.E 2002; the Cybercrimes Act 2015, the Electronic Transactions Act, the Human DNA Regulation Act, 2009; Law of the Child Act, 2009; the Law of Marriage Act, Cap.29 R.E 2002; the Penal Code, Cap. 16 R.E 2002; the Criminal Procedure Act, Cap. 20 R.E

[21] See eg *Kukutia Ole Pumbun and Another v Attorney General and Another* [1993] TLR 159; *Julius Ishengoma Francis Ndyanabo v Attorney General*, Civil Appeal No. 64 of 2001, Court of appeal of Tanzania, Dar es Salaam (Unreported); *Legal and Human Rights Centre and Others v Attorney General*, Miscellaneous Civil Cause No. 77 of 2005, High Court of Tanzania, Dar es Salaam (Unreported); *Christopher Mtikila v Attorney General*, Miscellaneous Cause No. 10 of 2005, High Court of Tanzania, Dar es Salaam (Unreported).

[22] Misc. Civil Cause No. 117 of 2004, High Court of Tanzania, Dar es Salaam (Unreported).

[23] The Court of Appeal of Tanzania had already considered this principle in the case of *Director of Public Prosecutions v Daudi Pete* [1993] TLR 22.

2002; the Bank of Tanzania Act, 2006, it contains provisions on protection of confidentiality and secrecy.

In contrast to the above pieces of legislation, the Electronic and Postal Communications (Consumer Protection) Regulations 2011 has elaborate basic principles of personal data protection which are found in international best practices. Regulation 6 states:

6.-(1) A licensee may collect and maintain information on individual consumers where it is reasonably required for its business purposes.
(2) The collection and maintenance of information on individual consumers shall be–
(a) fairly and lawfully collected and processed;
(b) processed for identified purposes;
(c) accurate;
(d) processed in accordance with the consumer's other rights;
(e) protected against improper or accidental disclosure; and
(f) not transferred to any party except as permitted by any terms and conditions agreed with the consumer, as permitted by any permission or approval of the Authority, or as otherwise permitted or required by other applicable laws or Regulations.

Apart from the general principles of the EPOCA, Consumer Protection Regulations govern collection and processing of personal information in electronic marketing (telemarketing). Regulation 7 states:

7.-(4) A licensee shall not engage in unsolicited telemarketing, sms-marketing and any other electronic methods unless -
(a) customer consents to the service;
(b) at the beginning of the communication, it discloses the identity of the licensee or other person on whose behalf it is made and the precise purpose of the communication;
(c) the communication gives out the breakdown of the total cost of any product or service that is the subject of the communication.

The EPOCA Consumer Protection Regulations provide principles of personal data regulation. However, these principles are only applicable to the electronic communication sector.

8. BVR and privacy regulatory vacuum

There is little in place in the current legislative framework for voter registration on privacy and data protection. As presented in Section 7 of this work, the only principle of data protection available in the Elections Act is the prohibition of disclosure of information about a voter. At the same time there is no specific data protection legislation in Tanzania. This leaves voters' personal data without adequate protection. The adoption of the biometric technology in the process of registration of voters creates greater potentials for violations of personal data than it was the case with the OMR technology. The Tanzania's scenario of BVR reflects the general tendency in the developing world, whereby the adoption of new technologies is rarely preceded by the adoption and implementation of robust regulatory

frameworks.[24] In these countries, critical assessments on impact of new technologies on human rights and the daily lives of individuals are also infrequent.[25] This failure means that the risks are not accessed and identified and thus corresponding risk mitigating measures are not implemented.[26]

There are several practices in Tanzania that are based on the use of personal information of voters. One of the uses of this information is making it available to other organisations (public or private) on a routine basis. This is against the principle of 'purposes specification' which requires that information that is collected for a particular purpose, in this case voting, should not be used for any other purpose without prior consent of the data subject who is the person whose information is undergoing processing. The purpose of voter registration is to allow citizens to exercise their basic political right to vote; it is not an information gathering exercise to be shared with other institutions, such as law enforcement authorities or for commercial interests.[27] In Africa, countries that have no national ID card system, use voter cards as generally accepted form of identification for business purposes.[28] In Ghana, for example, citizens use their voter cards for identification at local banks. The EC in Ghana argues that since voters voluntarily use the cards at banks, they thereby give permission for data to be exchanged between these institutions and the voters' roll database.[29] This is also the case in Tanzania where, private businesses as well as government offices require their customers to produce voter identification cards as a means of identification. This is due to the fact that, although Tanzania is undergoing national identification card registration, majority of its citizens have no national identification cards. As a result of this, these organisations frequently request verification of the information in the voter ID from the NEC.

There is also a tendency for candidates and/or their political parties to buy from voters their voting cards. This is corruption under the Elections Act. However, this practice has two main intentions. First, it intends to use the cards for voting to their favourable candidates. Second, even if no such cards are used for voting, the rationale is to reduce the votes of the opponent as in most cases voters' IDs which are sought to be bought belong to the opposition parties. In this particular case, personal information of voters becomes ordinary property exchanged in the market for money.

It is arguable that voter registration information stored in both paper and electronic formats must be sufficiently secured to prevent unauthorised access, to protect against unauthorised alteration or disclosure and to ensure that any legal requirements for information privacy are met.[30] The guiding principles that have been developed over time and have been widely accepted in different countries when adopting biometric voter register are thus summarised as follows:

> Ensure individuals have access to about their privacy and personal data rights, including by informing them upon collection of their data of the purpose and use of the data collected, as well as their right to access, correct and delete any data saved on their profile; limit

[24]Privacy International (n 11) 3.
[25]ibid.
[26]ibid.
[27]A Evrensel, 'Voter Registration in Africa: A Comparative Analysis', EISA (2010) <https://www.eisa.org.za/pdf/vrafrica.pdf> accessed 20 November 2016.
[28]ibid.
[29]ibid.
[30]ibid.

> authorised access to biometric data to specific actors, which access must be strictly based on the purpose for the collection, i.e. information collected for border management should only accessed by migration authorities; establish strict data retention permissions outlining the fixed time period for the destruction of each data set; develop secure physical and digital structure infrastructure; set up independent oversight and monitoring mechanisms to ensure accountability and responsibility of those collecting, storing and retaining biometric data.[31]

The above principles are minimum standards. The NEC may push for legislative reforms for these principles to be incorporated in the Elections Act.

9. Conclusion

The PNVR is a database of information for voters in Tanzania. The database is generated through the use of biometric technology. As the above discussion reveals, the voter registration process is governed by the URT Constitution and the national Elections Act. These sources of law which make the legal framework for voters in Tanzania do not provide for a regime of data protection. Beyond these two main sources, there is no law that provides anything for privacy in the PNVR. That notwithstanding, the Commission should inform people at registration if their information is to be made available to other organisations and should abstain from disclosing personal information of voters as captured in the register unless authorised by other laws.

Disclosure statement

No potential conflict of interest was reported by the author.

[31]Privacy International (n 11) 19.