



BIOMETRIC TECHNOLOGY, ELECTIONS, AND PRIVACY
INVESTIGATING PRIVACY IMPLICATIONS
OF BIOMETRIC VOTER REGISTRATION IN
KENYA'S 2017 ELECTION PROCESS.



Strathmore
UNIVERSITY

Biometric Technology, Elections, and Privacy

**Investigating Privacy Implications Of Biometric Voter
Registration In Kenya's 2017 Election Process.**

Dr. Robert Muthuri

Moses Karanja

Francis Monyango

Wanjiku Karanja

Acknowledgements

We would like to thank Privacy International for choosing to collaborate with us in this project and Strathmore School of Law for facilitating the survey on political messaging. We are very grateful to all those who responded to that survey. We also thank the following organizations for offering to shed light on their data management practices: Safaricom Ltd, Liquid Telecom, Independent Electoral and Boundaries Commission, National Cohesion and Integration Commission, The Communications Authority of Kenya and the Anonymous CSP. The following people who have also been invaluable to the efforts of making this report a reality: Betty Kendi, Grace Guyatu Diida, Isaac Rutenberg (Dr.), Luis Francesci (Dr.), and David Omondi.

List of Abbreviations

BCP	Business Continuity Planning
CA	Communication Authority of Kenya
CSP	Content Service Provider
EU	European Union
IEBC	Independent Electoral and Boundaries Commission
ISP	Internet Service Provider
KICA	Kenya Information and Communications Act
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
NCIC	National Cohesion and Integration Commission



Key Messages

- The Kenyan electoral law was amended to explicitly include biometrics (definition), biometric voter registration, biometric voter verification and biometric voter identification on the Election Day.
- There is no data protection legislation to operationalise the Article 31 right to privacy enshrined in the Kenyan Constitution. As such, there is no framework to protect the biometric and alphanumeric data in the voter register.
- A redacted version of the voter register is available for sale under the Access to Information Act.¹ This does not include the biometric data in the register. However, unsolicited political messages sent on behalf of political aspirants by Content Service Providers (CSPs), feature the alphanumeric data in the voter register. This ought to raise concerns of whether adequate mechanisms exist to protect the biometric and alphanumeric data in the voter register.
- The political messaging guidelines² prohibit CSPs from sending unsolicited bulk messages to customers who haven't subscribed for the service. CSPs should ensure that all recipients of political messages choose to opt-in to the service. However, our research shows that there was significant targeted political messaging during the campaign periods using an opt-out as opposed to an opt-in mechanism.
- Although the political messaging guidelines prohibit the unauthorised use, sale, of existing customer databases for purposes of sending out political messages, poll tracking and lobby activities, their enforcement was geared more towards preventing hate speech than protecting Kenyans biometric and voter data.
- People are aware that their right to privacy is being infringed but they feel helpless to react and do not know to whom or where to complain.
- A significant number of surveyed respondents said that they were opposed to receiving targeted political text messages but they do not seem to have adequate channels to report infringements of their privacy.
- The Communications Authority of Kenya (CA) does not have a centralised system to collect complaints. There also does not seem to be a dedicated mechanism for anonymous reporting of such complaints.
- Other bodies (private and public) are adopting the use of biometric data in their operations despite the lack of a data protection law.

1 No. 31 of 2016, Laws of Kenya.

2 Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Content via Electronic Communications Networks, July 2017.

Table of Contents

1. Introduction	1
2. Why did Kenya adopt biometrics in the elections?	2
3. What does privacy have to do with it?	4
3.1 Cambridge Analytica: was biometric data appropriated in micro-targeting?	5
3.2 The alleged IEBC hacking	6
4. Methodology	7
5. Findings	7
5.1 The legal framework	7
5.2 Survey on political messaging	9
5.2.1 Unsolicited political messages	9
5.2.2 Message content and location accuracy.....	11
5.2.3 Who sent the texts?	13
5.2.4 How do Kenyans feel about these unsolicited messages?	14
5.3 Interviews with stakeholders	15
5.3.1 Independent Electoral and Boundaries Commission (IEBC)	15
5.3.2 Safaricom Limited	17
5.3.3 Communications Authority of Kenya (CA).....	19
5.3.4 National Cohesion and Integration Commission (NCIC)	21
5.3.5 Liquid Telecom	21
5.3.6 Content Service Provider (CSP)	22
5.4 Summary	23
6. Discussion	24
6.1.1 No mechanism for ensuring consent is obtained.....	24
6.1.2 The lack of transparency	24
6.1.3 The lack of a data minimization culture	24
6.1.4 Deficiencies in data privacy law	25
6.1.5 Political messaging and internet advertising	25
6.1.6 Self - Regulation does not work	25
6.1.7 Resources are lacking	26
6.1.8 The General Data Protection Regulation (GDPR) and Vision 2030	26
6.1.8.1 Automated processing	26

References	28
Legal Instruments	28
Reports	28
Media Reports	28
Websites	29
Appendix I	30
Appendix II	33

1. INTRODUCTION

The use of biometric technology in political processes, i.e. the use of peoples' physical and behavioural characteristics to authenticate claimed identity, has swept across the African region, with other 75% of African countries adopting one form or other of biometric technology in their electoral processes. This has been necessitated in part due to the low trust majority of citizens have had with electoral management bodies and the assumptions that adopting such technologies will increase confidence and efficiency in the elections. This comes at a high cost to countries already struggling with expensive elections. Despite such costs, the adoption of biometrics has not restored the public's trust in the electoral process, as illustrated by post-election violence and legal challenges to the results of the 2017 Kenyan elections. However, this study only focuses on the privacy implications of adopting biometrics, an angle yet to be explored.

The Centre for Intellectual Property and Technology Law (CIPIT) conducted this research project to investigate the privacy implications of using biometric technology during the electoral process in Kenya. The project focused on two main questions: what are the motivations for the adoption biometric technology in the Kenyan elections and, how is privacy and security of personal data in Kenya impacted by the adoption of biometrics in the electoral system? We conducted primary and secondary research from our location in Nairobi, Kenya before, during and after the 2017 general elections. We will seek to contribute evidence-based research to academic, policy and advocacy engagements on population registrations, elections, data security, and privacy.

The key takeaway is that Kenya's legal landscape lacks the protections that should be demanded to safeguard Kenyans privacy and protect data. Transparency, trust and security is key when deploying biometrics and other data technologies. When such technologies are adopted in the absence of a strong legal framework and strict safeguards, they pose significant threats to privacy and personal security, as their application can be broadened to facilitate discrimination, social sorting and mass surveillance. The varying accuracy of the technology can lead to misidentification, fraud and civic exclusion. As such, it is crucial that the use of biometric technologies is regulated and their use scrutinized.

BIOMETRICS IN KENYA

Biometrics, according to section 2 of the Election Laws (Amendment) Act. 2016 are unique identifiers or attributes including:



Biometric technology collects stores and automates pattern recognition of unique biological or behavioural characteristics of individual subjects for purposes of identification. As shown in the figure above, these characteristics e.g. fingerprints, voice, or facial geometry are captured then matched with a person's data e.g. civic registration details i.e. name, gender, address, etc. During elections, a voter's fingerprint is captured, matched with their voter registration details and stored on the voting device for later use at a polling station when the existing database is compared with claimed identity for verification. Please refer to the complete infograph in Appendix II.³

3 Giulia Piccolino (2015): Infrastructural state capacity for democratization? Voter registration and identification in Côte d'Ivoire and Ghana compared, *Democratization*. <http://dx.doi.org/10.1080/13510347.2014.983906>

2. WHY DID KENYA ADOPT BIOMETRICS IN THE ELECTIONS?

After the disputed Kenyan 2007 election and the attendant violence, biometric technology was adopted for voter roll preparation and identification at polling stations. The main rationale for adopting biometric technology seems to have been to ensure a one-man one-vote election. The IEBC called for an audit after opposition leaders raised an alarm that they shared voter details with other Kenyans.⁴ 128,000 Kenyans or 0.8% of the voter register shared national IDs or passports. Keep in mind that when Kenyans kicked off the 2017 mass voter registration for the August 2017 General Election, there had been concerns that the integrity of the 2013 voter database had been breached post-election, and used by the ruling coalition to strategize on voter registration for the 2017 election.⁵

Following the promulgation of the 2010 Constitution, a new electoral legal regime was introduced, with amendments and harmonization of different laws relating to elections, management and political parties.⁶ Article 81 of the Constitution of Kenya thus provides that whatever electoral system the electoral body would adopt must be **simple, accurate, verifiable, secure, accountable, and transparent**. While these motivations may be honourable, the disastrous conducting of 2017's Presidential election and the role of technology will be analysed for many months even years to come. In the rush to employ the latest technology to solve problems with the electoral process, badly needed legal reforms have been neglected.

This project sets out an agenda for Parliament to begin to address weaknesses in Kenyan law when it comes to regulating technology, and recommendations that will strengthen the right to privacy and therefore the security of each Kenyan. The attendant history is therefore summarized in the infograph in Figure 1: The history of electoral biometrics in Kenya.

4 "128,000 voters share identification details, IEBC says", Daily Nation, 24th January 2017 <https://www.nation.co.ke/news/politics/128000-voters-share-ID-passport-numbers-IEBC/1064-3785274-u4xfly/>

5 Opposition cites Foul Play: <http://www.kahawatungu.com/2015/06/18/how-national-youth-service-nysis-being-prepared-for-future-election-riggings/>

6 See The Elections act 2011, The Political Parties Act 2011, and the IEBC Act 2011.

BIOMETRICS IN KENYA'S ELECTIONS

Tracing the journey of the adoption of the use of biometric technology in Kenya's electoral process

Kriegler Report

2007/8



The Kriegler Report on the causes of the post-election violence recommended an effective, transparent and efficient electoral system to ensure that elections are credible, free and fair.

The Constitution of Kenya (Promulgated)

2010

The new Constitution contained clear laws on how to conduct elections.

Art.38 states the right to free, fair and regular elections while Art. 81 and 82 requires the electoral commission to adopt a method that is simple, accurate and verifiable.



2011

The Elections Act

Biometric voter registration was made law in Section 13 of this Act. The use of technology in elections was also provided in Section 44 of this Act. This enabled the Biometric Registration of Voters (BVR) and Electronic Voter Identification (EVID).



2012

Biometric Voter Registration kits and process

The Election (Registration of Voters) Regulations were passed.

The Kenyan Government directly procured biometric voter registration (BVR) kits from Safran Morpho for USD 14,151,139.13.



The biometric voter registration exercise commenced towards the end of the year (2012) ahead of the March 2013 elections.

2013

General Elections



EVID kits were first used during the March 2013 elections. The kits comprised of a laptop and finger print scanner. The EVID process failed massively and IEBC had to rely on the manual register to identify voters.

Presidential Petition Elections

(Raila v IEBC) Petition No.5 of 2013. The question of what is a voter register was raised at the Supreme Court. The court held that a register is not a single document...a register "includes a register compiled electronically."



2017

General Elections



Election Laws were amended again (s.44A) to provide for a complimentary system of voter identification and transmission of results (manual transmission)

Election Laws Act (Amendment) 2016

Electoral law was amended to include definition of biometrics in Section 2, verification of biometric data before elections in Section 6A and an integrated electronic electoral system in Section 44.

Kenya Integrated Elections Management System [KIEMS]

The system combines biometric voter registration, electronic voter identification and electronic transmission of results.



KIEMS kits(tablets) were directly procured from Safran Morpho France for Ksh. 3.8 billion after cancelling the competitive tendering process.



During the August 2017 elections, the Kenya Integrated Electoral Management System(voter identification) worked relatively well compared to 2013 during the electronic voter identification process.

Figure 1: The history of electoral biometrics in Kenya

3. WHAT DOES PRIVACY HAVE TO DO WITH IT?

Indeed, biometrics databases compile and link multiple biometric identifiers. Although some databases can be used for legitimate purposes, there are many risks associated with storing the very information that constitutes an individual's identity. The misappropriation of this information can deny individuals their identity and lead to limits on personal freedom. In many countries, strong data infrastructure does not exist and as a result, deeply personal information is often leaked. Additionally, biometric data retention laws often do not specify the maximum storage length, further increasing the risk of database leaks and introducing new dangers. The greatest of which is perhaps scope creep: seeming benign biometric data stored in databases can later pose significant threats to civil liberties. Images stored by facial recognition technologies can identify different races. These applications raise concerns about discrimination, particularly in environments prone to social sorting.

The IEBC reported that 19.6 million Kenyans had registered to vote.⁷ Accordingly, the volume of personal data collected is huge, personal, specific, and valuable. How this collected data is stored, secured and accessed has serious ramifications on the human rights outcomes of such societies. A number of issues have been raised to date:

1. In the Auditor's report 2014/15,⁸ the Auditor questioned:
 - a. The transfer of 150 Electronic Voter Identification Systems (EVIDs) to Burundi. It is imperative to understand that a single EVID contains significant biometric data for the voters in a particular polling station. Even though the Commission argued that the EVIDs were 'cleaned' prior to being transferred, the Auditor responded that this was a sensitive matter and the Commission should have involved the stakeholders specified in its Act.
 - b. The transfer of 200 Biometric Voter Registers (BVRs) to the Ministry of Devolution. No details regarding these transfers and the purpose of the transfer were provided, a contravention of section 72(3) of the Public Finance Act, 2012. More importantly for us, what steps were taken to erase and ensure no data breaches occurred in the transfer process?
 - c. The loss of 48 BVRs in Egwen Constituency, Nandi County. These kits were actually stolen from the Kapsabet Warehouse, North Rift Region. The Auditor noted that in the circumstances, the security of data in terms of backup and control of unauthorised access of both machine and database might not be assured and confirmed by the Commission.
2. The IEBC also reported that some BVR kits had been stolen the Al-shabaab when the militant group attacked a police camp in Mandera East in January 2017.⁹

7 IEBC Statistics of Voters, Registered Voters Per County for 2017 General Elections, <https://www.iebc.or.ke/docs/Registered%20Voters%20Per%20County%20For%202017%20General%20Elections.pdf>

8 Report of the Auditor-General on the Financial Statements for National Government for the Year 2014/2015, http://www.oagkenya.go.ke/index.php/reports/doc_download/676-report-2014-2015

9 Al Shabaab steal BVR kits, guns, police car in Arabia police post raid, https://www.the-star.co.ke/news/2017/02/02/al-shabaab-steal-bvr-kits-guns-police-car-in-arabia-police-post-raid_c1499305

3. Opposition-led protests led to the previous Commission resigning from office and a new one appointed in its place.¹⁰ The resulting time constraints led to the amendment of the procurement, registration and audit timelines in the electoral law. The voter register had to be ready in 4 months instead of the previous 8 months. These constraints also justified the government's direct procurement and waiving of standard inspections to meet the timelines. Other amendments were therefore necessary to ensure a manual backup in case the technology failed. The standards inspection waiver was challenged in court to no avail in *Maina Kiai, Khelef Khalifa and Tirop Kitur vs IEBC & KEBS, Constitutional Petition 168 of 2017*.
4. There was a report that existing databases e.g. telecommunication subscriptions, population registers and voter registers, were used to engineer the outcomes of the elections by geographically targeting unregistered voters in certain regions and enlisting government officials to access the data and reach the target population.¹¹ It is also alleged that these data sets were also used to send specific personalized political messages to voters.¹²

3.1 Cambridge Analytica: was biometric data appropriated in micro-targeting?

In the wake of the Cambridge Analytica scandal,¹³ many Kenyans have been left wondering to what extent the firm was involved in the country. It is noteworthy that our studies in this project helped shed light on this issue and were featured on Channel 4¹⁴ and the New York Times.¹⁵ Our research findings in 5.2 Survey on political messaging below, show evidence of micro targeting on both sides of the political divide during the campaigns last year. We did not find any user of biometric data but alphanumeric data in the voter register featured in two forms of micro targeting:

- **Voter-turnout:** The first form of micro targeting was to encourage people to vote. This involved data mining techniques to profile people according to their supposed political affiliation. We posit that the data involved in such mining involved voter registration data particularly on the names and addresses of potential targets. In Kenya, such targeting is easier because peoples' names show their ethnic background. This subset of data was then combined with their telco messages asking them to vote for a particular candidate.
- **Voter registration:** Another form of micro targeting occurred to urge those who had not yet registered to vote to do so. This happened particularly during campaign period leading to the repeat presidential elections.¹⁶ First people were profiled geographically in line with their perceived voting blocs

10 Court allows CORD's anti-IEBC protests, warns against use of force <https://citizentv.co.ke/news/court-allows-cords-anti-iebc-protests-warns-against-use-of-force-125282/>

11 Revealed: Inside Jubilee's vote machine to beat Raila Odinga

<https://www.standardmedia.co.ke/mobile/article/2001228175/revealed-inside-jubilee-s-vote-machine-to-beat-raila-odinga>

12 Ibid.

13 Cambridge Analytica Uncovered: Secret filming reveals election tricks, <https://www.youtube.com/watch?v=mpbeOCKZffQ>

14 Kenyans bombarded with fake news in presidential election <https://www.youtube.com/watch?v=525TpQNmbAI&feature=youtu.be>

15 "Cambridge Analytica Had a Role in Kenya Election, Too", New York Times, 20th March 2018 <https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html>

16 "Revealed: Inside Jubilee's vote machine to beat Raila Odinga", Standard Newspaper, 4th February 2017 <https://www.standardmedia.co.ke/mobile/article/2001228175/revealed-inside-jubilee-s-vote-machine-to-beat-raila-odinga>

using civic registration details. They were then profiled electorally using their voter registration details to identify those who had not yet registered to vote. Finally, they were targeted with messages using their subscription details urging them to come out and register to bolster the numbers of the particular voting bloc in question.

It is noteworthy that Cambridge Analytica and its parent company have commenced insolvency proceedings¹⁷ after the multiple inquiries into their data-harvesting campaigns that compromised data of 87 million Facebook users.¹⁸ Even though this is seen as a business move to reconstitute as a different entity,¹⁹ it is a clear sign of the business and reputational consequences of losing the public's trust when an institution is not considered to be taking the protection of its users data seriously.

3.2 The alleged IEBC hacking

The memory is still fresh, the then presidential candidate Raila Odinga calling a press conference in the early hours of the morning alleging that the IEBC servers had been hacked and algorithm set to ensure an 11% difference favour of the then incumbent president Uhuru Kenyatta at all levels of results transmission. The CIPIT team investigated these allegations but was not able to establish claims based on the evidence presented and recommended a comprehensive audit of the system.²⁰

In fact, the introduction of biometrics technology was meant to ensure the credibility and trust in the electoral system. A hacking claim is therefore incredibly serious and could damage such credibility irreparably. The reason this accusation gained traction, without evidence, is in part due to the little knowledge available on how the system worked. How were the potential vulnerabilities in the transmission, storage and publication of results tackled? As technology becomes increasingly integrated into election systems and processes, it is imperative that it is well socialized to all the stakeholders at all points of the elections timeline, procurement, verification, polling, and post-election phases.

17 Cambridge Analytica and Scl Elections Commence Insolvency Proceedings and Release Results of Independent Investigation into Recent Allegations, 2nd May 2018, <https://ca-commercial.com/news/cambridge-analytica-and-scl-elections-commence-insolvency-proceedings-and-release-results-3>

18 Written testimony to the Fake News Inquiry, Brittany Kaiser <https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Brittany%20Kaiser%20Parliamentary%20testimony%20FINAL.pdf>

19 "Cambridge Analytica dismantled for good? Nope: It just changed its name to Emerdata", The Register, 2nd May 2018 https://www.theregister.co.uk/2018/05/02/cambridge_analytica_shutdown/

20 "Kenyan Elections and Alleged Hacking: A Look at the available evidence", CIPIT Blog, 18th August 2018 <http://blog.cipit.org/2017/08/18/kenyan-elections-and-alleged-hacking/>

4. METHODOLOGY

With the foregoing in mind, questions have been raised on the security of personal information in the IEBC voter register. At one point, it seemed that all one needed to know a particular individual's voter registration details i.e. their voter profile, was their ID number. One could therefore feed an ID/Passport number to the online portal²¹ or short code SMS (7000) and you would get the voter details (Name, polling station, county and ward). This made us wonder whether someone could harvest the data using data-driven bots. In addition, there was the question of who was providing the SMS service and the terms on which they were allowed access to the IEBC database. Did such access include the biometric data? Did such terms include privacy clauses to govern access, processing, and sharing of data? There was also the issue of political targeting via unsolicited messages to potential voters. We therefore sought to clarify the data management practices of the IEBC to determine how they protected biometric voter data. We resulted to a number of strategies to in this endeavour. We first reviewed the legal framework, mapped and interviewed the relevant stakeholders, and surveyed the voter population.

5. FINDINGS

5.1 The legal framework

Even without a data protection law, we are not entirely devoid of data protection law although not all are relevant to the use of biometric registration devices. Through Article 2 of the Constitution of Kenya, international conventions and declarations including the United Nation (UN) instruments become law in Kenya. The Universal Declaration of Human Rights (UDHR) 1948 states that *no one shall be subjected to arbitrary interferences with his privacy, family, home or correspondence, or to attacks upon his honour or reputation.*²² The International Covenant on Civil and Political Rights (ICCPR) 1996 reproduces this provision almost word for word.²³

The Constitution of Kenya in Article 31 states that every person has the right to privacy, which includes the right not to have (c) information relating to his or her family or private affairs unnecessarily required or revealed. The Elections (Technology) Regulations 2017 gazetted by the IEBC regulate the electoral technology being used by the Commission. Part V on Information Security and Data Storage requires the Commission to put in place mechanisms to ensure **data availability, accuracy, integrity, and confidentiality.**²⁴ Part VI provides for Data Retention, Disposal, and it states that the Commission for a period of three years after the results of the elections have been declared shall retain all electronic data relating to an election in safe custody. We presume that this is the information related to the election results and not that in the voter register. Unless the court orders otherwise, the data shall be archived in accordance with procedures prescribed by the Commission subject to the Public Archives and Documentation Service Act under the Kenya Information and Communications Act, 1998.²⁵

In July 2017, The Communications Authority of Kenya and the National Cohesion and Integra-

21 IEBC Voter Verification Portal <https://voterstatus.iebc.or.ke/>

22 Article 12, Universal Declaration of Human Rights

23 Article 17, International Covenant on Civil and Political Rights

24 Regulation No. 14, Elections (Technology) Regulations, 2017

25 Regulation No. 17, Elections (Technology) Regulations, 2017

tion Commission jointly issued The Guidelines for Prevention of Dissemination of Undesirable Bulk Political SMS and Social Media Content via Electronic Communications Networks. Clause 10.1. on unsolicited messages in the following terms:

CSPs SHALL NOT send unsolicited Bulk or Premium Rate Content to customers who have not subscribed for the service. CSPs shall ensure that all recipients of Political Messages have opted into the service. Such opt in will require the express consent of the recipients and opt-out procedures must be clearly notified to customers and kept functional at all times.

The guidelines also sanction unauthorised sharing of data in Clause 10.6 as follows:

Any unauthorised use, sharing or sale of existing customer databases for purposes of sending out Political Messages, Poll Tracking and lobby activities may lead to the immediate suspension of the inter-operability agreement between the CSP and the MNO or MNVO pending legal and/or regulatory determination.

However, the Guidelines still require MNOs, MVNOs, CSPs, and ISPs to strictly adhere to the law regarding the use of customer databases howsoever acquired.²⁶

This may be a reference to the Kenya Information and Communications (Consumer Protection) Regulations, 2010 under Kenya Information and Communications Act (KICA).²⁷ Regulation 17 on unsolicited communications requires consent of the subscriber in the following terms:

- (1) A person who uses automated calling systems without human intervention, facsimile machines or electronic mail for purposes of direct marketing without the prior consent of the subscriber commits an offence.

It also requires that a user be given the option to opt-in:

- (4) All automated direct-marketing schemes to be used in Kenya shall be based on an opt-in principle, in which potential subscribers shall be accorded the opportunity to accept or reject inclusion in a marketer's mailing list.

Regulation 15 on confidentiality requires that licensees i.e. telecom operators not to *monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data.*²⁸ It follows this with the re-assurance that: *..., nothing in this regulation shall be construed to mean that a licensee may sell or offer for free, to a third party, any information collected by the licensee without the prior consent of the consumer concerned.*²⁹

To conclude this section, the right to privacy established in the Kenyan Constitution is yet to be operationalised. The existing ICT laws and regulations recognise the necessity of user consent and opt-in mechanisms. A robust legal framework will establish all pivotal principles for data protection such as lawfulness, fairness and transparency, purpose limitation, data minimisation, data accuracy, storage limitation, and integrity and confidentiality.

26 Clause 8, The Guidelines for Prevention of Dissemination of Undesirable Bulk Political SMS and Social Media Content via Electronic Communications Networks, 2017.

27 No. 2 of 1998

28 Regulation 15(1), the Kenya Information and Communications (Consumer Protection) Regulations, 2010.

29 Regulation 15(3), the Kenya Information and Communications (Consumer Protection) Regulations, 2010.

5.2 Survey on political messaging

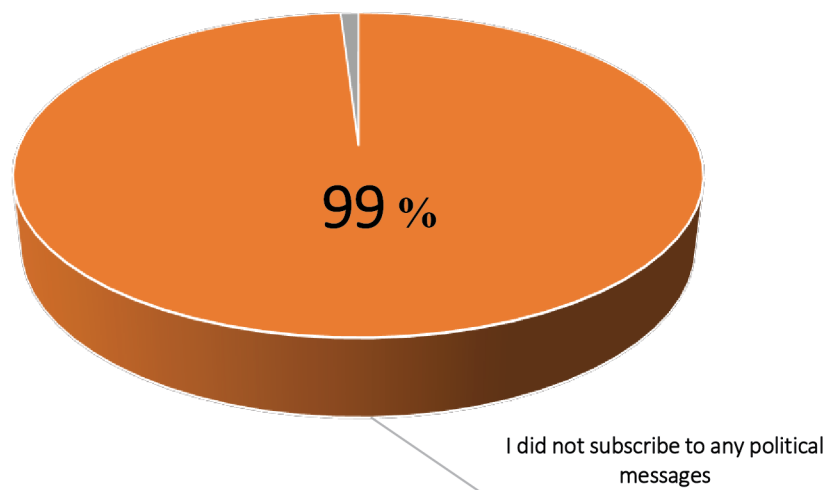
We designed a survey to investigate whether the voter register was in any way appropriated to profile and disseminate undesirable political SMS content via electronic communications networks. This was to clarify reports that individuals got campaign texts from candidates during the period before elections.³⁰ These texts were accurate as to where the individuals were voting and to some extent, possible political inclinations. Our objectives were two-fold to understand, a) how widespread the political messaging was across the country, and b) how personalized the political messaging texts were, c) the candidate categories that were being campaigned for, and d) the service providers that sent out the messages. What follows is a discussion of the survey results. To begin with, this was an online survey distributed among law school students. We received responses from people registered in 35 of the 47 counties in Kenya with 228 receiving unsolicited text messages.

5.2.1 Unsolicited political messages

A vast majority of campaign messages sent to voters during the 2017 election period were unsolicited. Furthermore, a majority of voters did not provide politicians with their phone numbers as part of a political message subscription service or for any other related purpose. This illustrated in our survey of 228 voters on political messaging during the 2017 election period as follows:

99% of the 228 respondents had not subscribed to any political messaging service, yet received unsolicited political campaign messages (Question 8).

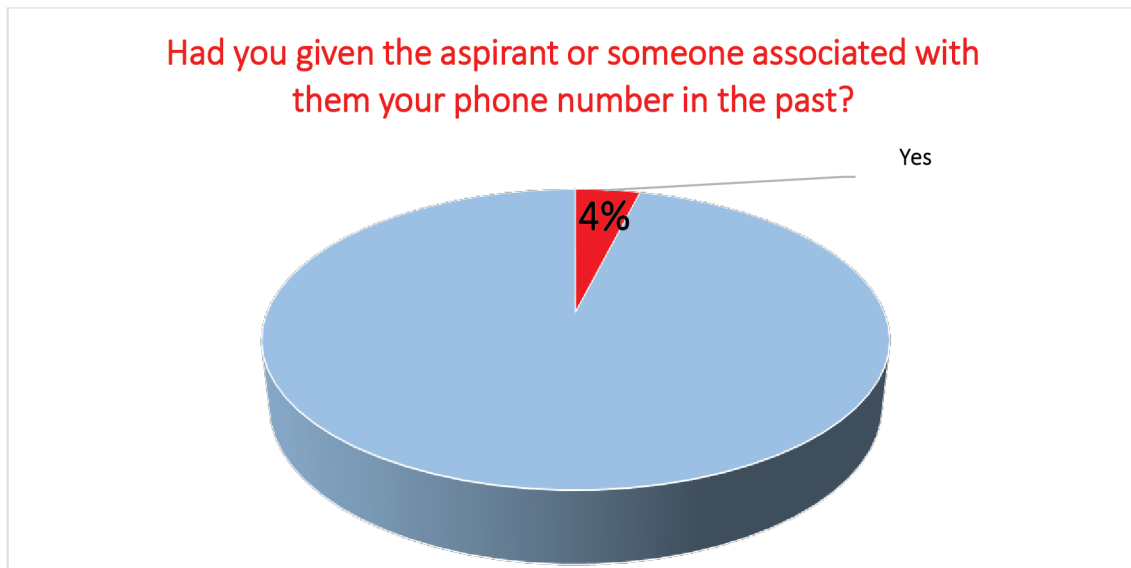
Had you subscribed for such message(s)?



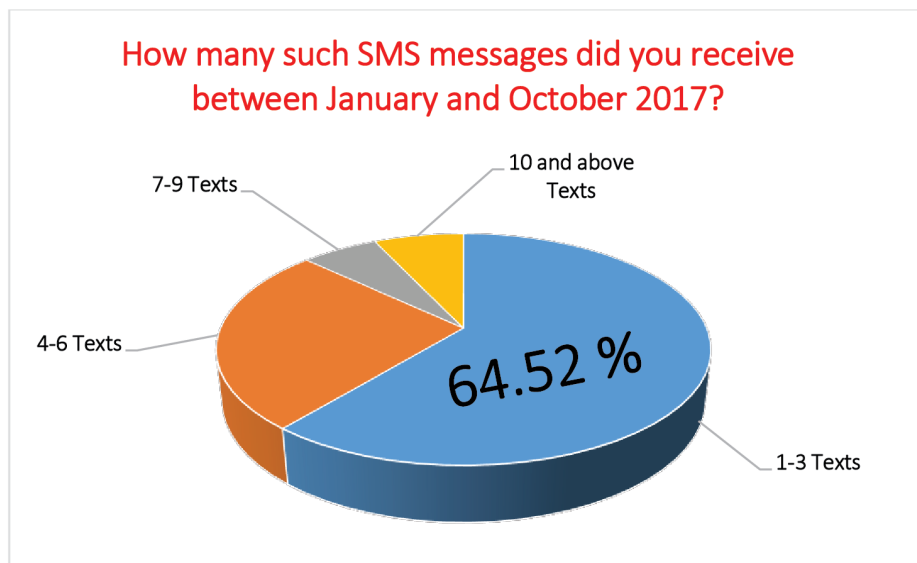
Similarly, of the 228 respondents that received unsolicited texts, only 4% had given their numbers to political aspirants (Question 6).

30 "Revealed: Inside Jubilee's vote machine to beat Raila Odinga", Standard Newspaper, 4th February 2017 <https://www.standardmedia.co.ke/mobile/article/2001228175/revealed-inside-jubilee-s-vote-machine-to-beat-raila-odinga>

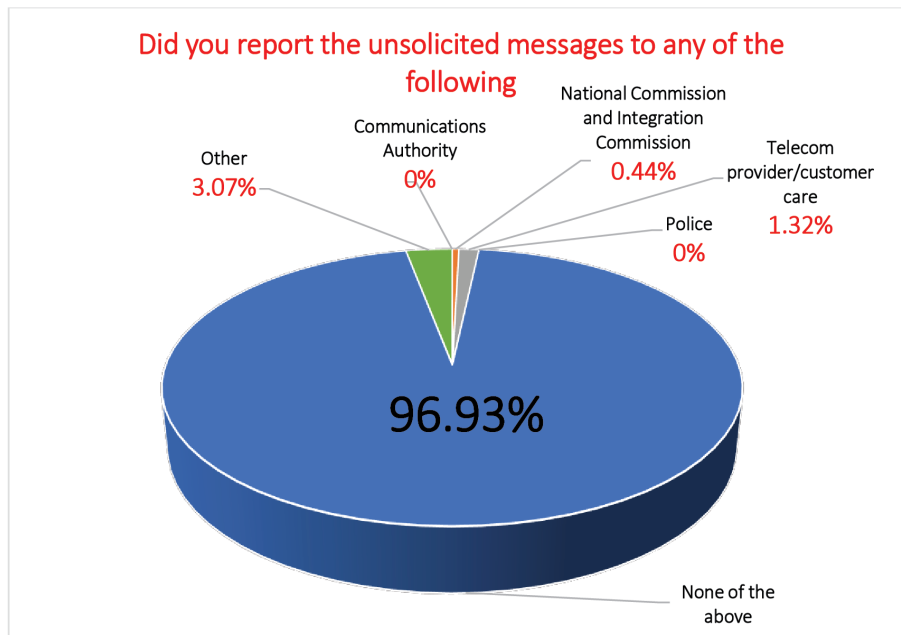
64% of respondents received 1-3 text messages during the 2017 election period (Question 7).



These statistics line up with an account of an interviewed CSP, who while speaking on condition of anonymity, stated that MNOs stipulated that CSPs were only allowed to send a maximum of 3 messages to one individual.



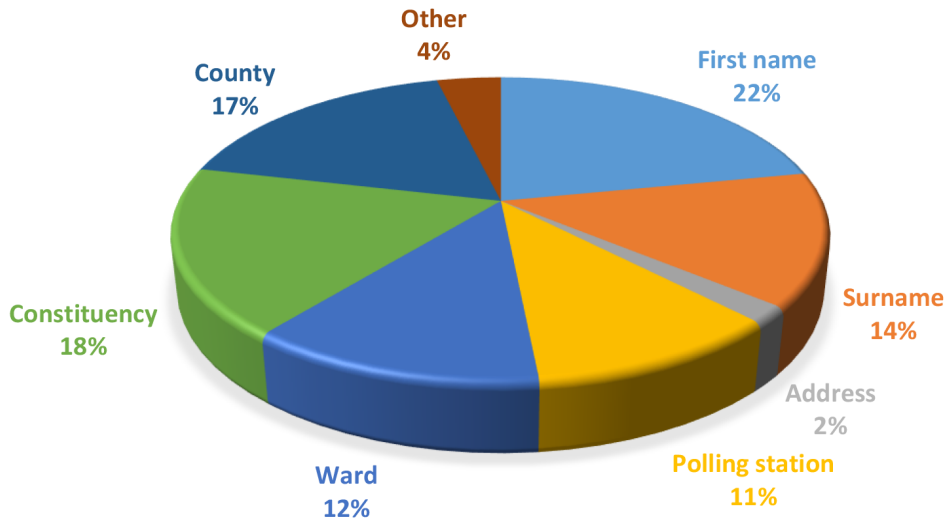
Unfortunately, 97% of respondents did not report these messages to relevant authorities such as the Communications Authority of Kenya (Question 9). It could be that voters did not know the appropriate forum(s) for the reporting of unsolicited messages. It may also indicate apathy amongst voters with regard to the capacity of regulators to enforce against such actions of politicians.



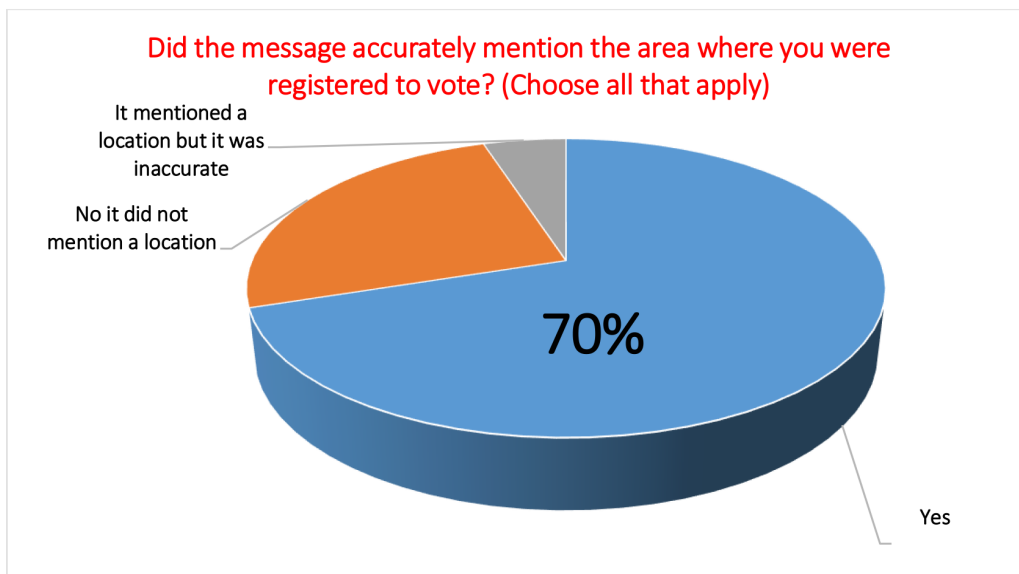
5.2.2 Message content and location accuracy

The messages sent to the respondents frequently contained information that identified the name, or voting location of the respondent. (Question 4)

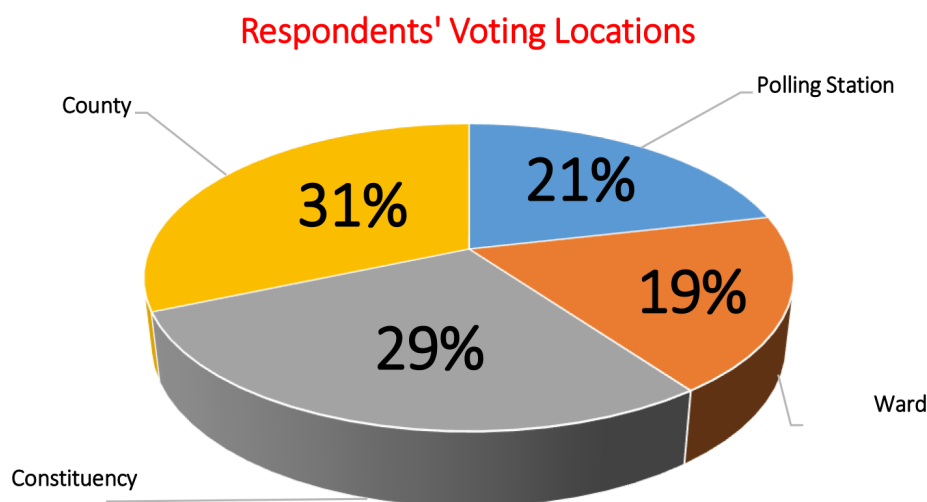
Did the SMS include any of the following information about you?



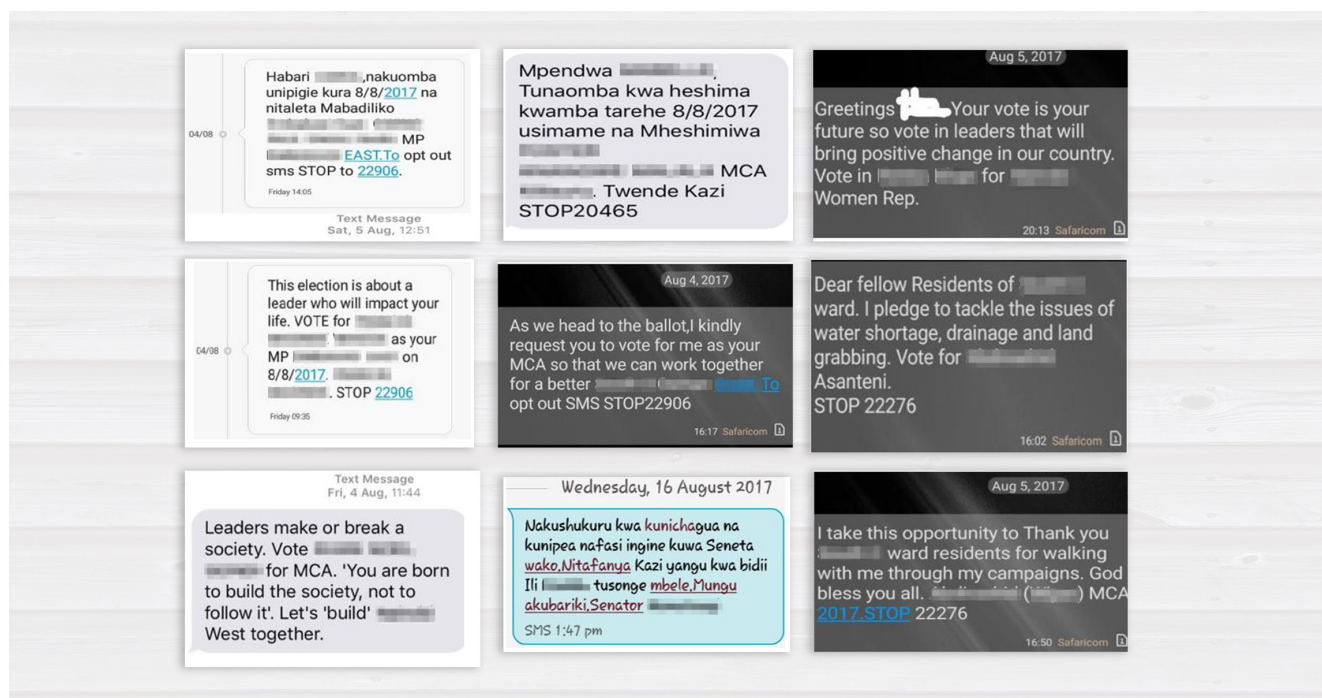
Likewise, 70% of the respondents stated that the messages targeting them accurately identified their voting location. (Question 10)



These messages identified the respondents voting locations in the following proportions (Question 10):

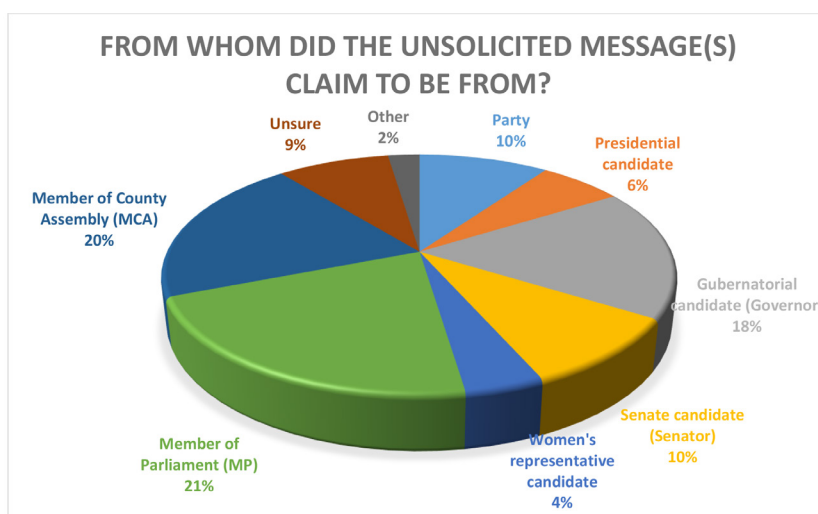


In addition to the survey, we asked respondents to send us a screenshot of the messages they had received. While many chose not to do so, or had already deleted the messages in question, 30 did so. These messages served as an indicator of the reliability of the answers to the survey, as well as giving some indication of the breadth of the issue. The following is a sample of campaign messages received by the respondents (Question 12).



The accuracy of the SMS messages received, particularly in regard to the respondents' voting location, leads to questions as to where this data was achieved. Given that one clear source of this data could have been the electoral register, has this been compromised in respect of the voters' personal data? Similarly, does this raise concerns as to the security of voters' biometric data also? Additionally, these statistics may point to the level at which voters' personal data was compromised and used by politicians to send unsolicited campaign messages to the respondents.

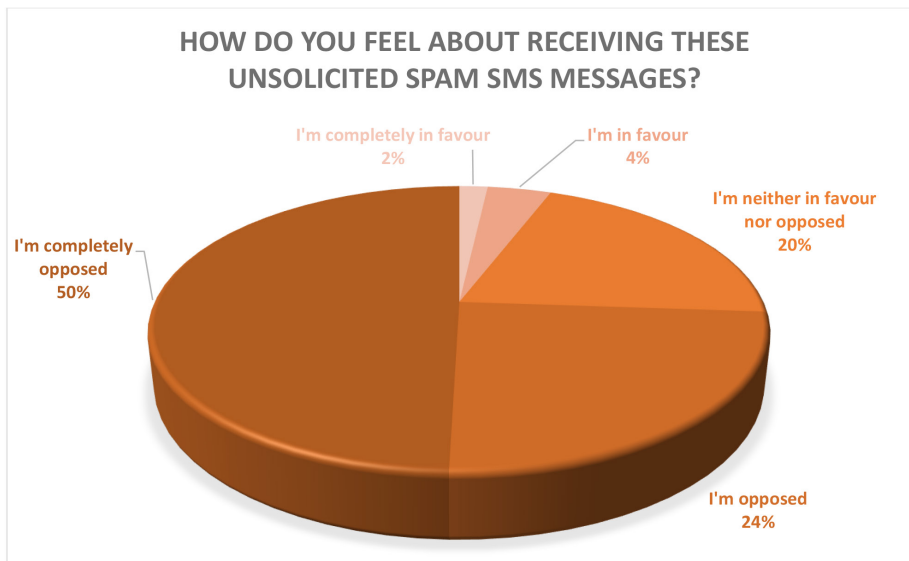
5.2.3 Who sent the texts?



Respondents received campaign messages from political candidates in the following proportions: (Question 5)

5.2.4 How do Kenyans feel about these unsolicited messages?

74% of Kenyans are opposed to receiving unsolicited campaign messages. (Question 11)



The majority of respondents indicated that they did not know how their data was obtained for use in election campaigns. They expressed concerns as to the means used by the political parties and candidates to obtain their phone numbers and personal data without their consent. Some respondents expressed their wish for the enactment of laws that would protect their data privacy. Here is a sample of what they said:

- *The spam texts circulated since nominations. I find it important for you to find out how those involved in the nominations got access to the data.*
- *I am concerned as to where the aspirant got my number considering I do not reside in my voting area. If the contact was obtained through IEBC should I be worried about my data protection!*
- *After the research, do use your findings to do something that will help the electorate get better future elections.*
- *Are they hacking. So it means that our records at IEBC aren't safe?*
- *It felt intrusive because I don't know where they got my personal information.*
- *Even private numbers and entities are now messaging in an unsolicited manner on WhatsApp as well as SMS. The telecom providers shouldn't disclose our information.*
- *I received a call from a person claiming to be from the chief's office asking if I had been registered as a voter. The person was calling me all the way from my upcountry yet I have lived all my life in Nairobi with the occasional visits to my upcountry.*
- *Law should be in place so as not to send such political messages, without consent.*
- *Such messages should be sent to people that have consented. Consent is very essential*
- *Data protection laws are long overdue.*

The foregoing raises a number of questions:

1. How many versions of the register exist and which version of the register is accessible to the public?

2. Who can access the voter register and what level of detail are they allowed to access?
3. Who has access to the biometric voter data?
4. Who has the permission to alter the biometric voter register?
5. Were the political messaging guidelines followed by CSPs, and MNOs?

5.3 Interviews with stakeholders

We interviewed a number of stakeholders to expound on the established legal framework to help clarify the foregoing findings in the survey.

5.3.1 Independent Electoral and Boundaries Commission (IEBC)

Given the significant number of respondents that had received unsolicited text messages, we wondered whether information from the voter register had been appropriated in such endeavours. We visited the IEBC secretariat and learnt that one could present an Access to Information request³¹ for the voter register via a letter to the CEO giving justification for the register. This acknowledges that the voter register is a public document. We initially wanted to put in such a request but we were exhorted to model the data minimization principle to collect as little data as possible and only if necessary. Nevertheless, we learnt that the version of the register that we would have acquired in this instance would be redacted to the name, electoral area, and truncated ID number showing the first two and last two digits. We sought further clarification as to the data management practices of the IEBC presented below.

The IEBC balances the *right of access* with the voter's *right to privacy*. Most of the requests are by researchers, universities, or students but people interested with or affiliated to politics also make requests particularly in the pre-election period. However, it is not possible for one to opt-out of being included in the register for sale. The IEBC explained that the software cost implications would not allow this to happen.

The IEBC clarified that there is only one register i.e. the *Principal Register* under the Elections Act of 2011. However, it has several components including the *Constituency Register* and the *County Register*. The IEBC receives a comprehensive registration form when a voter is registering including the voter's phone number. They emphasised this is purely for the Commission's internal use. They acknowledge they would need the voters' consent before releasing their phone numbers.

Collection of Biometric Data

Fingerprint data is collected (all 10 fingers) together with the voter's alphanumeric data i.e. name, age, disability, polling station, county, constituency, etc. This information is collected continuously but halted during election petitions, general elections, and referendums. Mass voter registration is carried out to "hype up" voter registration and to support the continuous registration. Data is collected at the polling station level, at registration centres, using stand-alone biometric data kits. This data is backed up on flash disks, which are then taken to and uploaded onto a server at the constituency level/regional level, after which it is transmitted to the central database at the IEBC headquarters. The IEBC saves voter registration data both continuously and periodically. Uploading of data to the IEBC central database is done, via a secure network owned by the IEBC: fortnightly in the case of continuous voter registration, and weekly (at county level) in the case of mass voter registration.

31 Access to Information Act, No. 31 of 2016.

Processing Data

Biometric data collected at the polling station level, at registration centres, is captured in its raw form. Prior to its upload on the central database, every piece of data (biometric and corresponding alphanumeric data) undergoes **deduplication** (matching) to countercheck if it is similar to any other record already stored in IEBC's system. If it is found to be similar to data already stored on the system, it is put under a **suspension account** awaiting further investigation.

Alteration of Data

Constituency registration officers are in charge of their constituency's register. They hold the reference data and thus compare voter records with the reference data to ensure that there is no duplicity. They also assign a polling station to the data collected. This data is then transmitted to the central database where it is matched with the national register of persons to ensure that the voter's national identity numbers are valid. In the event of errors in the voter registration data, the voter has the option to fill a **change of particulars form** after which the registration officer makes amendments to the records based on that form. In this case, the biometric data remains the same but alphanumeric data is amended at the constituency server. In the event that a voter's details are missing from the register, he voter has the option to fill a **claim form** after which their biometric details are recaptured so that they are included in the register. In the event that a voter transfers their polling station, the voter has the option to fill a **transfer form** after which the Constituency Registration Officer effects changes in the database by amending the records to show the change. In the case of deceased voters, on receipt of records from the births and deaths registry, the deceased voter's records are **deactivated** so that another party does not use that voter's record to vote. The IEBC notes that this is controversial because the civil registry's births and deaths records are not very accurate e.g., an audit of the national register by KPMG found that 92,000 deceased persons still have active voter records. When IEBC ran this data against candidates' data, a number of candidates were flagged as dead while they were still alive! KPMG then revised their data to 86,000 deceased persons. The IEBC therefore notes that it is important to improve data sharing between the IEBC and the civil registry to improve accuracy.

Access to Data

On the issue of what procedures had been put in place to protect access to the biometric data, the IEBC confirmed that there were elaborate firewalls and pass codes for one to access the information. Only duly authorised IEBC officials could access the information and the specific process was on a need to know basis. The IEBC is in charge of this process and not the software vendor. There are various levels of access to biometric data as follows:

- *Clerks who capture the biometric data at voter registration centres have very limited access. They only key in the data and cannot alter the data.*
- *Constituency registration officers can amend alphanumeric data to correct mistakes or deactivate a deceased voter's account. This is limited to their specific constituency register.*

- County ICT officers have a **maintenance account**.
- The manager in charge of data at the IEBC headquarters can view actions carried out to all data across the IEBC voter registers. They **cannot however alter data** and must refer any alteration request to the relevant constituency registration officer. The **Director of ICT similarly has slightly more access to the data** but cannot amend or alter the data.
- The **biometric software vendor** grants the rights to view and access the data. The software vendor cannot alter the data.

Data Storage

The biometric voter registration kits belong to the IEBC. They are stored in a secure location once voter registration is complete. The IEBC continuously tests their systems to identify weaknesses. They further conduct system audits to ensure that that system is secure. The IEBC database has not been hacked to date. The IEBC emphasize that the system has not been hacked to date because data storage is not centralised, i.e. the IEBC uses both primary and secondary servers. It also confirmed that it maintains an **external disaster data recovery site**, which accords with section 25(1) of the Elections (Technology) Regulations 2017. However, they could not disclose whether this site was located within the Kenyan jurisdiction as that information is confidential.

The IEBC is not aware of the presence, nor has it received reports of voter registers in the public domain listing voters' phone numbers. The IEBC believes that the right to privacy needs to be protected especially in light of biometric data, which is sensitive. This is the reason why the IEBC voter register does not display voters' ID card numbers or biometric data.

It is noteworthy that The IEBC is currently aware of the sensitivity of biometric data and that is why they do not include it in the register available for sale. However, this position cannot be guaranteed in the future and ought to be secured in a legislative framework.

5.3.2 Safaricom Limited

We further sought clarification from Safaricom as to their role and interaction with CSPs during the political campaigns and their data management practices in general.

Safaricom notes that their role of MNOs is only with respect to bulk SMS content pushed through a licensed CSP and not the normal peer-to-peer messages sent by subscribers over the network. To this end, a political party/politician wishing to send a bulk political message would need to approach the CSP. The CSP would then send the message to an MNO for approval prior to its dissemination. In the event that the MNO is not able to determine whether the planned message is inflammatory, inciteful, hateful or a violation of the law, the message is escalated to the NCIC for further vetting in line with the National Cohesion and Integration Act. Receipt of the message is expected to be on an **opt-in basis** and unsolicited messages are prohibited. It is important to note that the Guidelines only apply to **bulk messages** and do not cover peer-to-peer messages, noting that MNOs have no visibility over the actual content of the later sent through their respective networks.

Access to Subscription Data

Safaricom's subscriber data is kept secure and confidential, and subject to strong access control.

- **Agents** and **dealers** who register subscribers on behalf of Safaricom are also bound to keep the information they collect for onward transmission to Safaricom secure. Non-compliance may result in contract termination as well as criminal sanctions under KICA.
- **Law enforcement agencies** may in very specific circumstances prescribed under law be provided with subscriber data, including but not limited to KICA, Prevention of Terrorism Act and National Intelligence Service Act e.g. for purposes of criminal investigations or prosecution under Section 27A (2) and (3) of KICA.

Outside of the limited obligations to share subscriber data as prescribed under law, we only share subscriber data with the **express consent of the customer**. We do not share subscriber data with CSPs, who from time to time send premium rate and bulk messages to subscribers. Safaricom has also taken the further step of independently verifying from customers any subscription requests to premium rate services offered by CSPs. In instances of unsolicited messages from CSPs, a customer may opt to complain to Safaricom for contractual action, or better still to the CA for regulatory action as the CA independently licenses CSPs.

Biometric Data

Safaricom has recently launched the use of voice biometric data to assist in customer operations. This is a pioneer service that we hope will improve the customer experience on our network and offer an enhanced customer service. The procedures for protecting this data will mirror the standards used to store all Safaricom data with the relevant security features.

Protecting Data

Safaricom notes that even in the absence of a data protection law, it is bound by law and license conditions to safeguard subscriber data. These include, but are not limited to-

- a. Protection to every person's privacy, as enshrined in Article 31 of the Constitution, including privacy on one's communications [Article 31(d)]
- b. Duty to keep subscriber data safe and secure and to only make disclosure as prescribed under law, detailed in Section 27A (2) and (3) of KICA.
- c. Duty to keep subscriber data safe and secure, as detailed in Regulation 15 of Kenya Information and Communications (Consumer Protection) Regulations, 2010.
- d. Strict confidentiality provisions in Safaricom's operating licenses.

In addition to this, Safaricom and other stakeholders continue to advocate for a com-

prehensive data protection to be put in place. By virtue of the above, Safaricom takes a number of measures to ensure compliance with legal and license requirements to safeguard subscriber data that include: -

- a. a dedicated network and cybersecurity team;
- b. documented processes and procedures for handling of subscriber data that is secured by storing strong access controls, and disciplinary action against staff that do not comply;
- c. routine audit procedures to make sure that any requirements improvements / corrective action is taken;
- d. Compliance to the ISO27001 & ISO22301 standard with respect to information security and BCP respectively.

As seen above, Safaricom has expanded into voice biometrics to enhance its customer experience. The National Transport and Safety Board (NTSA) is looking to introduce smart driving licenses that will feature the driver's blood group so the blood group is known immediately in case of an accident.³² Increasingly more institutions, both public and private, are demanding different forms of biometric data from Kenyans. In many circumstances, there is no option to opt-out. For instance, if you decline to have your photo taken, you will not get the sim card.³³ It cannot be gain said that Kenyans are innovative and are looking to monetise their data-driven business models. The urgent support from government is therefore necessary via a robust data protection framework so that innovators can earn the trust of Kenyans.

5.3.3 Communications Authority of Kenya (CA)

The CAs enforcement role against non-complying parties to the CA and NCIC guidelines was a central part of our study. This was in response to the high proportion of voters who received unsolicited campaign messages from politicians. This not only points to inadequacies in the guidelines but also raises concerns as to CA's regulatory capacity vis-a-vis these guidelines as well as the potential comprise of sensitive personal data such as biometrics.

Access to Subscription Data

Regulation 4 of the Kenya Information and Communications (Consumer Protection) Regulations stipulates that all automated direct-marketing schemes used in Kenya shall be grounded on an **opt-in principle**. The reality on the ground does not reflect this provision as seen in the CSPs revelation that most SMS had **opt-out** options. This coupled with the fact that a vast majority of respondents (99%) stated that they had not subscribed to any campaign subscription service indicates that these "subscription" services are operating in contravention of the law (Question 8).

32 How NTSA's Smart Driving License Promises to Change Kenya's Roads

<http://www.techweez.com/2017/07/11/ntsa-smart-driving-license-kenya-roads/>

33 Pre-programmed smart phones to augment Safaricom's photo IDs drive

<http://www.nairobibusinessmonthly.com/pre-programmed-smart-phones-to-augment-safaricom-photo-ids-drive/>

In situations where the law is flouted in this manner, the law prescribes a penalty of a fine not exceeding **three hundred thousand shillings** or to imprisonment for a term not exceeding three **years or both**. The Authority is of the view that this penalty is too low in most cases. Therefore, they have in consultation with the Attorney General's Office, sought to amend this provision through amendments to the parent Act and the subsidiary legislation. Moreover, they are also exploring proposals from the public for the revocation of infringers' licenses, particularly of those who contravene the public's right to data protection and privacy. These amendments are however yet to be enacted.

Protecting Data

In the absence of a data protection law, the CA is mandated³⁴ to ensure that customers give express consent for the dissemination and use of any personal any service provider that is licensed by the Authority. Similarly, restrictions on disclosure of information held by the CA is implemented pursuant to Article 35 of the Constitution, which protects the right of access to information. Data privacy and protection is therefore inextricably linked to the CA's consumer protection role.

The CA, as such, has a complaints mechanism, whereby on the receipt of consumer complaints, the same is escalated to the Authority's cybersecurity unit. This unit works in conjunction with other agencies, including enforcement agencies, to analyse the complaint and prescribe an appropriate response such as a "takedown".

These procedures however ultimately fall short in the absence of a data protection law. This is evidenced by lack of reporting of unsolicited messages to the Authority (Question 9). The lack of a data protection law creates a lacuna as to the parties responsible for ensuring that collected personal data is protected. The onus of protection is thus shifted to the consumer, which is impractical in light of the widespread ignorance as to the appropriate parties to report such misuse of data.

A data protection law is imperative for CA to effectively carry out its mandate in this respect.


34 Regulation 3 of the Kenya Information and Communications (Consumer Protection) Regulations.

5.3.4 National Cohesion and Integration Commission (NCIC)

The NCIC did not receive complaints from the public vis-à-vis unsolicited political campaign messages that they received during the election period in 2017. They however received fifty-six (56) complaints of hate speech along ethnic/tribal lines. This is reflective of their mandate to encourage national cohesion and integration by outlawing discrimination on ethnic grounds under the National Cohesion and Integration Act (No. 12 of 2008). This mandate is reflected in section 13.4 of the CA and NCIC guideline.

The Commission indicated that the CA and NCIC guidelines had been effective with regard to ensuring that bulk messages did not contain hate speech or inciting language. MNOs would forward to the Commission messages submitted to them by CSPs. The NCIC then reviewed the messages, within 48 hours, to determine if they contained hate speech. NCIC would approve messages free of hate speech, which would then be disseminated by MNOs to their recipients.

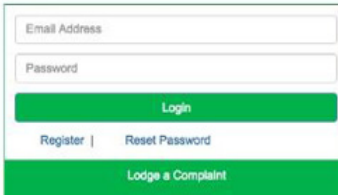
The NCIC also has a complaints channel through which members of the public are able to report incidences of hate speech including those on social media or received via messaging services. Complaints received in June – December 2017 have resulted twelve (12) arrests & arraignments & One (1) conviction.




NATIONAL COHESION AND INTEGRATION COMMISSION KENYA
PAMOJA

Below are a list of complaints you can lodge to NCIC

1. Ethnic discrimination
2. Discrimination by way of victimization
3. Comparison of persons of different ethnic groups
4. Harassment on the basis of ethnicity
5. Discrimination in employment
6. Discrimination in membership of organizations
7. Discrimination by other agencies
8. Discrimination in access to and distribution of public resources
9. Discrimination in property ownership, management and disposal
10. Hate speech
11. Offence of ethnic or racial contempt



Email Address
Password
Login
Register | Reset Password
Lodge a Complaint



Toll Free SMS line
15666

You can also reach us on:-
National Cohesion and Integration Commission
KMA Center, 6th Floor, Mara Rd, Upper Hill
P. O. Box 7055-00100 Nairobi, Kenya
Tel. +254-20-2585702/3/1
Email: info@cohesion.or.ke
Website: www.cohesion.or.ke

The CA and NCIC guidelines have as such been largely effective with respect to preventing dissemination of hate speech. This is in contrast to their effectiveness in preventing the unauthorised use of voters' personal data in subscription services. The NCIC sentiments in this regard support the enactment of a comprehensive data protection law in light of the sensitive data collected by the IEBC, MNOs and the NCIC itself.

5.3.5 Liquid Telecom:

Liquid Telecom raises pertinent questions as to the protection of subscription data namely: the scope of the data to be protected and the ownership of this data. In this sense, this telco underscores the importance of a data protection law that clearly defines what constitutes as data, and the scope of the ownership of such data, to ensure that it is protected at the right juncture.

Biometric Data: Liquid Telecom does not currently collect any of their clients' biometric data. The scope of clients' personal data is limited to identifying data, including but not limited to; clients' names, addresses and contact information.

Access to subscription data: This is limited depending on the role of the requestor and the purpose for which they require the data. For example, the Finance team's access is limited to data required for billing purposes. The foundation of this model is the contracts entered into by Liquid Telecom and their clients that set out how the data will be handled and by which parties.

Protecting Data: While Liquid Telecom stores subscription data in an outsourced system, this system is protected by an inbuilt security system whereby the security of the data is enmeshed with the security of the system.

Alteration of subscription data: Clients can change their data at the time of subscription through a self-service portal in which they enter their data. Liquid Telecom's staff can also alter client's data on the client's behalf. This is through an elaborate process whereby the client must submit a duly filled and signed change request form, which is then reviewed by the company's legal department and approved by either the chiefs of teams (depending on the data in question) or the CEO.

5.3.6 Content Service Provider (CSP):

Approximately 97% of the respondents did not report the unsolicited text messages that they received (Question 9). This is supported by an interview with a CSP, whom speaking on condition of anonymity, revealed that most texts could not be replied to and other texts had **opt-out** options instead of **opt-in**.

Access to subscription data: The CSP indicates that they complied with MNOs conditions for the sending of bulk SMSs via MNOs systems. In particular, the CSP stated that they, after obtaining information from politicians as to the content of the texts, would fill out the message's content in a form and send this form to the MNO for approval. Texts in vernacular or that contained inciting language or hate speech were however not approved.

Protecting Data: The CSP suggests that the onus of acquiring recipients' consent for inclusion in the subscription service fell on politicians. They do not as such ask politicians the source of the mobile numbers provided to them. The CSPs are thus relegated to a mere conduit of the messages from the politician to the MNO and on to the recipients. Their role in protecting subscribers' personal data appears to be non-existent. They further reveal that they did not oblige to requests politicians due to their contractual obligation to protect their clients' data.

This raises questions as to the source of phone numbers used to send voters unsolicited campaign messages. The CSPs in response to this question point to inadequacies in the implementation of the CA and NCIC guidelines that enable politicians to obtain phone numbers without voters' consent. Moreover, the CSP suggests that voters' information, including their personal data, can be obtained from the IEBC.

5.4 Summary

- The Kenyan electoral law was amended to explicitly include biometrics (definition), biometric voter registration, biometric voter verification and biometric voter identification on the Election Day.
- There is no data protection legislation to operationalise the Article 31 right to privacy enshrined in the Kenyan Constitution. As such, there is no framework to protect the biometric and alphanumeric data in the voter register.
- A redacted version of the voter register is available for sale under the Access to Information Act.³⁵ This does not include the biometric data in the register. However, unsolicited political messages sent on behalf of political aspirants by Content Service Providers (CSPs), feature the alphanumeric data in the voter register. This ought to raise concerns of whether adequate mechanisms exist to protect the biometric and alphanumeric data in the voter register.
- The political messaging guidelines³⁶ prohibit CSPs from sending unsolicited bulk messages to customers who haven't subscribed for the service. CSPs should ensure that all recipients of political messages choose to opt-in to the service. However, our research shows that there was significant targeted political messaging during the campaign periods using an opt-out as opposed to an opt-in mechanism.
- Although the political messaging guidelines prohibit the unauthorised use, sale, of existing customer databases for purposes of sending out political messages, poll tracking and lobby activities their enforcement were geared more towards preventing hate speech than protecting Kenyans biometric and voter data.
- People are aware that their right to privacy is being infringed but they feel helpless to react and do not know to whom or where to complain.
- A significant number of surveyed respondents said that they were opposed to receiving targeted political text messages but they do not seem to have adequate channels to report infringements of their privacy.
- The Communications Authority of Kenya (CA) does not have a centralised system to collect complaints. There also does not seem to be a dedicated mechanism for anonymous reporting of such complaints.
- Other bodies (private and public) are adopting the use of biometric data in their operations despite the lack of a data protection law.

35 No. 31 of 2016, Laws of Kenya.

36 Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Content via Electronic Communications Networks, July 2017.

6. DISCUSSION

6.1.1 No mechanism for ensuring consent is obtained

It is evident from the foregoing findings that CSPs were able to send bulk-personalised messages to potential voters without their consent. One of the plausible explanations that has been fronted is that this data came from mobile money agents. However, such registers do not feature voter registration data. It has also been suggested that this data may have come from MNOs. Again, subscription data does not feature voter registration data. The other explanation fronted was that the civic register was used to first profile the voter geographically then subscription data was used to reach out to them. This can explain why some people got calls from their home area chiefs even though they had since moved from their rural setting. However, that it is also evident that different IEBC personnel have access to the biometric voter register at constituency, county, and national levels. Only the IEBC has voter registration data, which was included in the messages that we collected in the survey.

It is possible that political aspirants were able to obtain this data from the rogue officials at the Commission. More mechanisms that are stringent are therefore necessary regarding access to the biometric voter register. Access should not be limited to who can alter data. It should also be viewed from the perspective of who can export, print or view significant parts of the register. Only a limited number of personnel should have a list view of the register. Additionally, printing or exporting rights should be extremely limited. A significant number of personnel have access to the register so, as of now, it is difficult to pinpoint the particular personnel that may have leaked data from the IEBC.

6.1.2 The lack of transparency

The interviews were limited by confidentiality clauses. We therefore need an escrow institution empowered to keep the industry accountable in their data management practices. It is evident that public bodies, corporates, social media platforms have had the means but little incentive to self-regulate. There have been calls for expanding the right of access in a manner that could allow for educators, journalists, activists and academics to investigate corporates in a manner that helps civil society keep the corporate world accountable. There has also been calls for improving enforcement and the budget for data protection authorities. It is likely that Parliament will nominate The Commission on Administrative Justice to oversee the data protection framework. Whichever regulation results, it ought to ensure utmost transparency. We should therefore work towards accountable algorithms. The AI and blockchain Taskforce should chart the way forward on how Kenyan developers can join the accountable algorithms movements. Using Kenyans' personal information without their authorization to profile them is legally, morally, and ethically wrong.

6.1.3 The lack of a data minimization culture

After much contemplation, we determined not to buy the voter register or access versions of the register readily available from CSPs in the market. Our survey results help to disprove the notion that Africans do not care about privacy. 74% of our respondents said they were opposed to such political targeting. However, we need to inculcate the data minimization principle in our culture. There is also a case to be made that instead of the huge investment made in biometric technology every election cycle, it makes more sense to invest and maintain the civic register from which the IEBC can draw from when necessary. This would also be more cost effective as the civic register handles births and deaths and can therefore avail a more consolidated approach of updating the voter register.

6.1.4 Deficiencies in data privacy law

Contrary to some perceptions, Kenya is not entirely devoid of privacy legislation. As we have seen, our Constitution guarantees the right to privacy in Article 31. A cursory view of the Kenya Law Reports case law shows considerable litigation on this provision. Kenyans should therefore not shy away from enforcing their right to privacy using judicial channels. Nevertheless, we do need a stronger legislative and regulatory framework to enforce and operationalize this right. The data leaks associated with India's Aadhaar Scheme³⁷ is a prime example of the detrimental consequences of a lack of strong and comprehensive data protection laws.

The foregoing studies show that the political messaging guidelines were treated as such, guidelines! A more robust framework to protect Kenyans privacy and protect them from the monetization of their data.

6.1.5 Political messaging and internet advertising

The 2017 electoral campaigns saw a hoard of political messaging and information controls in the form of misinformation, disinformation, and outright fake news. The political messaging guidelines were only effective in controlling hate speech messages; they did not prevent the profiling and political messaging of voters. Relatedly, Paul Olivier Dehaye, in his testimony to the Digital, Culture, Media and Sport Committee of members of the British parliament,³⁸ told the Committee that the psychographics we have experienced through Cambridge Analytica happened on an individual level; convincing someone to change candidates based on their psychological profile. The bulk of Cambridge Analytica's techniques however, focus more on a collective effect – the ability to spread rumours. He notes that this is probably easier to generate leveraging our impulse to share information and only Facebook is in a position to investigate the impact that this had on an election. A more rigorous legislative framework is necessary to curtail this invasive and subversive practice.

6.1.6 Self-Regulation doesn't work

In the wake of the Cambridge Analytica Scandal, it has become evident that privacy policies and related industry standards are not effective in protecting users' data. Prior to the scandal, social media platforms had been highly trusted domains. However, they have not applied their enforcement mechanisms including audits of external developers to ensure data was not being misused.³⁹ Direct state regulation may also be extreme, exposing users' data to the excesses of government agencies. A co-regulatory model that combines self-regulation⁴⁰ with government oversight will ensure that social media platforms and public bodies collecting user data abide by their commitments. This calls for a strong regulatory data protection authority with tenure and adequate powers to police the industry. This should include the power to audit the data management practices of corporates and issue escalated fines as deemed necessary. This is the current practice in jurisdictions that we aim to emulate e.g., UK, Germany, Italy, Australia, and Canada.

37 The Aadhaar Scheme is a unique identifier system comprising the identity and biometric information (fingerprints, iris scans) of more than 1.1 billion registered Indian citizens in the form of 12-digit individual identification numbers. In January 2018 it was reported that some of the biometric data from the Aadhaar Scheme was on sale online. <https://www.medianama.com/2018/05/223-aadhaar-leaks-list/>

38 Guardian News, Cambridge Analytica whistleblower Christopher Wylie appears before MPs <https://www.youtube.com/watch?v=X5g6IJm7YJQ>

39 "'Utterly horrifying': ex-Facebook insider says covert data harvesting was routine", The Guardian, 20th March 2018 <https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas>

40 "A Regulatory Framework for Facebook and Other Platforms Is Already in Place", D-zone, 27th March 2018 <https://dzone.com/articles/a-regulatory-framework-for-facebook-and-other-plat>

6.1.7 Resources are lacking

Whatever entity is determined to oversee data protection regulation; it will need significant resourcing if it is to succeed in policing the industry. In his testimony to the Digital, Culture Media and Sports Committee of the British Parliament, Cambridge Analytica whistle-blower Christopher Wylie showed empathetic criticism for the lack of technical resource at the UK's Information Commissioner's Office to understand how relational databases and machine learning works yet they are in charge of regulating data.

6.1.8 The General Data Protection Regulation (GDPR) and Vision 2030

We need to study the big data ecosystem from both technical and regulatory perspectives ensuring we welcome their potential while being wary of their risks, particularly for our fragile economy and democracy. The Kenyan government has consistently underlined Information Technology Enabled Service –Business Process Outsourcing (ITES-BPO) as a flagship project for Kenya's Vision 2030.⁴¹ This is a data-intensive business model that involves offshoring non-core computer work. This business model will be affected by the GDPR; which bars transfer of EU data to jurisdictions without adequate safeguards for data protection. The GDPR is finally coming into force later this month i.e. 25th May 2018.

6.1.8.1 Automated processing

The GDPR is also strongly opposed to automated processing, particularly of sensitive personal data e.g. financial, health, or insurance data. This is because EU citizens do not want computer algorithms deciding important issues concerning their lives without human oversight. Equally, Kenyans have a right to be informed of the opt-out options to such processing.

⁴¹ This is the country's development programme from 2008 to 2030. It was launched on 10 June 2008 by President Mwai Kibaki. Office of Public Communications.

7. CONCLUSION

This project has explored the historic motivations for adopting biometric technology. Kenya was motivated to invest in biometric technology in order to solve several problems that have plagued the electoral process. There must not be doubt in the minds of Kenyans that elections have been conducted properly. Firstly, biometric voter registration would ensure an accurate voter register. Biometric verification at the polling station would ensure one person one vote, and the results could be transmitted to IEBC, avoiding any tampering. However, there was minimal understanding of how the technology worked which exacerbated the claims that the system was hacked during the voter transmission and tallying exercise on 9th August 2017. We therefore sought to investigate the data management practices of the IEBC to determine how the biometric and alphanumeric data in the voter register was protected. We analysed the legal framework, engaged the relevant stakeholders and sought the views of Kenyans, the owners of the data in question.

The foregoing research shows that the right to privacy is well established in the Kenyan Constitution but there is no legal framework to actualize this right. CSPs targeted Kenyan voters with political messages that featured the alphanumeric data in the voter register. There was no evidence that the CSPs accessed the biometric data but the fact that there are no protections is undesirable and harmful when it falls into the wrong hands. We have seen that self-regulation does not work, we need a concrete mechanism anchored in legislation for MNOs and CSPs to prove that users have granted their consent. We also need more transparency via a strong Data Protection Authority with the power to issue escalated fines and with a sufficient right of access to help keep the industry accountable. This Authority will also work to inculcate a culture of data minimisation in the Kenyan society. The Authority should also be resourced sufficiently to ensure the Kenya is ready for the GDPR, a key determinant to the success of the BPO-ITES projects of Kenya's Vision 2030.

8. RECOMMENDATIONS

In conclusion, we recommend a strong data protection framework that constitutes the following modules:

- **Data protection legislation:** The sale of personal data is big business in Kenya as there is no law against such practices. Kenya is in dire need of a comprehensive data protection law that will ensure citizens have a say over the use of their data by bodies that collect them;
- **Data Protection Authority:** bodies that collect personal information are not accountable to anyone and there is need of a data controller to enforce accountability on the use of data collected from people.
- **Capacity building:** the foregoing findings and discussion call for significant resources to be invested in the proposed Data Protection Authority in such a way that it will be able to raise awareness and police social media platforms, CSPs, corporates and public institutions.

REFERENCES

Legal Instruments

1. Universal Declaration of Human Rights 1948
2. International Covenant on Civil and Political Rights 1966
3. Access to Information Act, No. 31 of 2016
4. The Elections Act 2011
5. Elections (Technology) Regulations, 2017
6. Elections (Technology) Regulations, 2017
7. Elections Act of 2011
8. IEBC Act 2011
9. The Political Parties Act 2011
10. The Guidelines for Prevention of Dissemination of Undesirable Bulk Political SMS and Social Media Content via Electronic Communications Networks, 2017.
11. Kenya Information and Communications (Consumer Protection) Regulations, 2010.

Reports

1. Giulia Piccolino (2015): Infrastructural state capacity for democratization? Voter registration and identification in Côte d'Ivoire and Ghana compared, Democratization. <http://dx.doi.org/10.1080/13510347.2014.983906>
1. Report of the Auditor-General on the Financial Statements for National Government for the Year 2014/2015, http://www.oagkenya.go.ke/index.php/reports/doc_download/676-report-2014-2015
2. Written testimony to the Fake News Inquiry, Brittany Kaiser <https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Brittany%20Kaiser%20Parliamentary%20testimony%20FINAL.pdf>

Media Reports

1. "‘Utterly horrifying’: ex-Facebook insider says covert data harvesting was routine", The Guardian, 20th March 2018 <https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas>
2. "128,000 voters share identification details, IEBC says", Daily Nation, 24th January 2017 <https://www.nation.co.ke/news/politics/128000-voters-share-ID-passport-numbers-IEBC/1064-3785274-u4xfly/>
3. "A Regulatory Framework for Facebook and Other Platforms Is Already in Place", D-zone, 27th March 2018 <https://dzone.com/articles/a-regulatory-framework-for-facebook-and-other-plat>
4. "Cambridge Analytica dismantled for good? Nope: It just changed its name to Emerdata", The Register, 2nd May 2018 https://www.theregister.co.uk/2018/05/02/cambridge_analytica_shutdown/
5. "Cambridge Analytica Had a Role in Kenya Election, Too", New York Times, 20th March 2018 <https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html>

6. "Kenyan Elections and Alleged Hacking: A Look at the available evidence", CIPIT Blog, 18th August 2018 <http://blog.cipit.org/2017/08/18/kenyan-elections-and-alleged-hacking/>
7. "Revealed: Inside Jubilee's vote machine to beat Raila Odinga", Standard Newspaper, 4th February 2017 <https://www.standardmedia.co.ke/mobile/article/2001228175/revealed-inside-jubilee-s-vote-machine-to-beat-raila-odinga>
8. Cambridge Analytica and Scl Elections Commence Insolvency Proceedings and Release Results of Independent Investigation into Recent Allegations, 2nd May 2018, <https://ca-commercial.com/news/cambridge-analytica-and-scl-elections-commence-insolvency-proceedings-and-release-results-3>
9. Cambridge Analytica Uncovered: Secret filming reveals election tricks, <https://www.youtube.com/watch?v=mpbeOCKZFfQ>
10. Court allows CORD's anti-IEBC protests, warns against use of force <https://citizentv.co.ke/news/court-allows-cords-anti-iebc-protests-warns-against-use-of-force-125282/>
Guardian News, Cambridge Analytica whistleblower Christopher Wylie appears before MPs <https://www.youtube.com/watch?v=X5g6lJm7YJQ>
11. How NTSA's Smart Driving License Promises to Change Kenya's Roads <http://www.techweez.com/2017/07/11/ntsa-smart-driving-license-kenya-roads/>
<http://www.nairobibusinessmonthly.com/pre-programmed-smart-phones-to-augment-safaricom-photo-ids-drive/>
12. Kenyans bombarded with fake news in presidential election <https://www.youtube.com/watch?v=525TpQNmbAI&feature=youtu.be>
13. Opposition cites Foul Play: <http://www.kahawatungu.com/2015/06/18/how-national-youth-service-nysis-being-prepared-for-future-election-riggings/>
14. Pre-programmed smart phones to augment Safaricom's photo IDs drive

Websites

1. IEBC Voter Verification Portal <https://voterstatus.iebc.or.ke/>
2. IEBC Statistics of Voters, Registered Voters Per County for 2017 General Elections, <https://www.iebc.or.ke/docs/Registered%20Voters%20Per%20County%20For%202017%20General%20Elections.pdf>
3. Medianama.com <https://www.medianama.com/2018/05/223-aadhaar-leaks-list/>



POLITICAL MESSAGING SURVEY

Survey on political messaging during the 2017 election period

The Centre for Intellectual Property and Information Technology (CIPIT), is a research centre at Strathmore Law School. We're conducting research on the privacy implications of applying biometric technology to Kenya's 2017 election process. As part of that we're trying to understand how personal data collected via the Biometric Voter Register (BVR) kits was handled. Particularly, if it helped in sending unsolicited spam SMSs via telecommunication networks. By using the term unsolicited, we mean that you did not sign up to receive such messages. This is not research about political bias or hate speech so we're not interested in what political party or aspirant sent the message. We're only concerned with whether your consent was sought in line with the political messaging guidelines issued jointly by the Chairman of the National Cohesion and Integration Commission and the Director General of the Communications Authority. So kindly participate to help us characterize and formulate policy considerations with regard to the adoption of biometric technologies and their impact on your privacy and security. Finally, we respect your privacy so we commit to only use the information collected for purposes of the study and to destroy it at the end of this project in June 2018. In thanks for your endeavours responding to this survey, your entry will draw for one of 30, Kshs. 1000 vouchers which can be spent on Jumia!

* 1. When did you register as a voter?

- Before 2012
- 2012
- 2017
- I'm not registered to vote

2. In what county are you currently registered to vote?

* 3. Did you receive unsolicited spam SMSs from a political aspirant, and urging you to vote for them?

- Yes
- No

4. Did the SMS include any of the following information about you?

- | | |
|--|---|
| <input type="checkbox"/> First name | <input type="checkbox"/> Ward |
| <input type="checkbox"/> Surname | <input type="checkbox"/> Constituency |
| <input type="checkbox"/> Address | <input type="checkbox"/> County |
| <input type="checkbox"/> Polling station | <input type="checkbox"/> Other (please specify) |

5. From whom did the unsolicited message(s) claim to be from? (tick all that apply)

- | | |
|---|---|
| <input type="checkbox"/> Party | <input type="checkbox"/> Women's representative candidate |
| <input type="checkbox"/> Presidential candidate | <input type="checkbox"/> Member of Parliament (MP) |
| <input type="checkbox"/> Gubernatorial candidate (Governor) | <input type="checkbox"/> Member of County Assembly (MCA) |
| <input type="checkbox"/> Senate candidate (Senator) | <input type="checkbox"/> Unsure |

Other (please specify)

6. Had you given the aspirant or someone associated with them your phone number in the past?

- Yes
 No

7. How many such SMS messages did you receive between January and October 2017?

- 1-3
 4-6
 7-9
 10 and above

8. Had you subscribed for such message(s)?

- I subscribed to some political messages but got other unsolicited messages
 I did not subscribe to any political messages
 I subscribed to all political messages I received

9. Did you report the unsolicited messages to any of the following?

- Communications Authority
- National Commission and Integration Commission
- Telecom provider/customer care
- Police
- None of the above
- Other (please specify)

10. Did the message accurately mention the area where you were registered to vote? (Choose all that apply)

- Yes, my polling station
- Yes, my county
- Yes, my ward
- No it did not mention a location
- Yes, my constituency
- It mentioned a location but it was inaccurate

11. How do you feel about receiving these unsolicited spam SMS messages?

- I'm completely in favour
- I'm opposed
- I'm in favour
- I'm completely opposed
- I'm neither in favour nor opposed

12. If you would like to send us a screens hot of any text messages you received during the campaign, this would be very helpful for our research. We will not disclose information about your location, county, or your name or number. If you would like to do this, please send a screenshot via whatsapp or forward the message to 0777342048.

13. Is there anything else you would like us to know?

14. If you'd like to participate in the draw, kindly provide a number or email to enable us reach you.

BIOMETRICS IN KENYA

Biometrics, according to section 2 of the Election Laws (Amendment) Act, 2016 are unique identifiers or attributes including:



fingerprints



voice



DNA



earlobe geometry







retina and iris patterns



hand geometry

Unregulated biometric data collection exposes one to:

- Identity theft 
- Misuse of personal information 
- Unauthorised distribution and sale of data 
- Financial Loss
- Personal privacy erosion 



Remedies

- There is dire need for a data protection law to stipulate clearly on how personal information being collected by data processors is going to be processed and used.
- There is need to give the data subjects more say on the collection of their personal information and its use.
- There is need for transparency from data processors on how they handle and use personal information and data.

Research by CIPIT, Strathmore University & Privacy International..

Source: Biometric Technology, Elections Management & Privacy in Kenya Report

www.cipit.org







OUR CONTACTS

CIPIT: Strathmore Law School
3rd Floor, SR. Thomas More Building,
Madaraka Estate, Ole Sangale Road
Nairobi West Area, City Square , Nairobi.
P.O Box 59857 - 00200 Nairobi, Kenya
Tel: (+254) (0)703-034612



Strathmore
UNIVERSITY