A VERY SECRET BALLOT

Lucy Purdon

• *A case study on the electoral process in Kenya* •

ABSTRACT

This essay focuses on elections in Kenya and analyses the use of technology and the exploitation of personal data in both the electoral process and campaigning. We only need to look to Kenya's election history to understand why it is important. The 2007/2008 election resulted in violence that killed over 1,000 people and displaced over 600,000. The 2013 election was relatively peaceful, but marked the rise of online "hate speech" that exploited ethnic tensions. The 2017 election result was annulled and rerun amidst great tension and a death toll of at least 33 people, while targeted online political adverts played on national fears of further violence. The essay concludes with an outline of the expected minimum protections and safeguards, which can be applied globally.

KEYWORDS
Kenya | Election | Voting | Politics | Biometric | Technology | Data | Profiling | Adverts | Campaigning | Targeted | Hacking | Security | Databases | Misinformation | Propaganda | Data protection | Data analytics

2018 is a bumper election year: Brazil, Colombia, Mexico, Pakistan, Zimbabwe and reportedly Thailand are due to have either general or presidential elections. The security and transparency of electoral processes is under global scrutiny. From the rushed adoption of biometric voter registration, the concerns over the security of voter registers and voting systems themselves, all the way to the phenomenon of targeted political advertising and misinformation campaigns on social media, there is much to distract voters from the single most important democratic question: Who will best represent you and your country?

This essay focuses on elections in Kenya and analyses the use of technology and the exploitation of personal data in both the electoral process and campaigning.

We only need to look to Kenya's election history to understand why analysis of the topic is important. The 2007/2008 election resulted in violence that killed over 1,000 people and displaced over 600,000. The 2013 election was relatively peaceful, but marked the rise of online "hate speech" that exploited ethnic tensions. The 2017 election result was annulled and rerun amidst great tension and a death toll of at least 33 people, while targeted online political adverts played on national fears of further violence.

This essay is based on an investigation by Privacy International during the 2017 presidential elections into the origins of two controversial online campaigns and the involvement of western data analytics companies.[1] This essay also draws on research published by the Centre for Intellectual Property and Information Technology (CIPIT) at Strathmore University in Kenya, in partnership with Privacy International, analysing the adoption and implementation of biometric voter registration.[2] In addition, the essay reflects the advocacy and policy work undertaken by Privacy International following the Facebook/Cambridge Analytica scandal that unfolded in March 2018, which again put the spotlight on Kenya's 2017 election.

1 • Biometric voter registration

When the Kenyan government announced the adoption of biometric voter registration (BVR) and authentication in the 2011 Elections Act, the motivations were reasonable. The recommendation to move to a new registration system was made by the Kriegler Commission, which was set up to investigate the Kenyan electoral system following the post-election violence of 2007/2008.[3] The Kriegler Commission's report also provided a technical note on the features of biometric voter systems.[4]

It was thought that a BVR system, including voter fingerprints, in addition to verification at the polling station, would ensure one person one vote and avoid accusations of irregularities at the ballot box. The results could be transmitted directly to the electoral body, avoiding any tampering. There were concerns that votes were being cast on behalf of dead people who were still on the voter register. The Kriegler Commission estimated there were "probably" 1.2 million deceased persons included in the register in 2007,[5] but there are no available numbers to support the claim that votes were being cast on their behalf either in that election or subsequent elections. This concern continued with George Morara, chairman of the Kenyan National Commission on Human Rights (KNCHR) saying prior to the 2017 election that "In Kenya, people say the dead come back to vote, and then return to their graves."[6] But, was there an alternative, less expensive and intrusive solution than a BVR? Would a reformed birth and death register have solved the problem? This was never discussed.

Before embarking on such data intensive and potentially intrusive initiatives, governments need to ask, why do this at all? What problem is a biometric database, for example, trying to solve? How will it succeed? What are the consequences if it fails?

One major concern is that governments are keen to implement initiatives that collect a lot of personal data, but lack consideration for securing the personal data those projects generate. Biometric systems are one example of data-intensive systems that are potentially very intrusive. The concern from human rights advocates in South Africa, for example, is that when these systems are adopted in the absence of strong legal frameworks and strict safeguards, biometric technologies pose grave threats to privacy and personal security, as their application can be broadened to facilitate discrimination, profiling and mass surveillance.[7] Another concern is that the varying accuracy and failure rates of the technology can lead to misidentification, fraud and civic exclusion, a central factor in the ongoing challenges we are currently seeing played out in India's Supreme Court regarding the Aadhaar biometric scheme currently underway in India.[8]

In the case of Kenya, the technology failed massively during the 2013 election, and polling stations had to rely on the manual register to identify voters. In 2017, the system performed relatively well compared to the 2013 debacle,[9] but as this essay will explore, the extent to which biometric technology has improved the credibility of democracy and Kenyan elections is still a contested claim, given a variety of other factors.

2 • Security of voter databases

Voter registration databases are often poorly secured and vulnerable. Data breaches occur globally, and the numbers involved are staggering. The personal information of over 93 million voters in Mexico,[10] including home addresses, were openly published on the internet after being taken from a poorly secured government database. This can be highly sensitive information given the context; in Mexico for instance up to 100,000 people are reportedly kidnapped each year.[11] Similarly, the personal information of over 55 million Filipino voters were made publicly available online, the biggest data breach in the Philippines' history.[12]

Research undertaken in Kenya to uncover whether the 2017 voter database was shared with third parties – and if so by whom – revealed the register was openly available for sale with no protections or safeguards. Consequently, voters received unsolicited text messages from candidates, identifying the receiver by name, constituency and even local polling station.[13] Already, we see that these technological applications are far from restoring much needed trust.

3 • The problem with the lack of data protection

Kenya does not have a comprehensive data protection law which would compel any entity – public or private – to respect fundamental data protection standards. This would include detailing what is collected, the purpose of collection, how it will be stored and with whom it will be shared. Under new data protection laws in Europe for example, entities must also provide the legal basis for collection and obtaining informed consent from the individual, in particular for the processing of sensitive personal data, such as biometric data. Without appropriate data protection laws, individuals are left vulnerable to excessive data being collected about them, without their consent and used in ways they are not aware of. When companies collect data in countries with insufficient legislation and share it with third parties, it is unclear what standards they, and these third parties, are holding themselves to, if any. Where data is generated, individuals should be able to find out which organisations and companies hold what kinds of data about them and what they use it for. Having a law on the books is one thing, but it must also be effectively implemented. An essential part is an independent authority which is properly resourced and able to investigate complaints.

Would data protection have helped the situations outlined in this essay? It might have made the Kenyan government think twice before implementing the system the way they did. It would make it easier for Kenyans to exercise their rights and get answers, such as finding out what data was collected, how it was used, how long it was stored, and with whom it was shared.

The next two sections explore this issue in a different context.

4 • Misinformation and Propaganda

In countries across the world, the spread of misinformation and propaganda during election time has been a problem for decades, however it received little international attention or concern. Frustratingly, when it recently became a problem in the United States of America (US) during the 2016 presidential election and also in Europe around Brexit, it suddenly had a title: "fake news".[14]

The second decade of the 21st century saw social media hailed as sparking revolutions and bringing about democratic change.[15] But less attention was paid to the political and social tensions amplified by the same spaces. Silicon Valley failed to predict, comprehend or even attempt to understand what was happening around the world, nor heed repeated warnings that content designed to stir up ethnic tension posted on their platforms had a real world effect. In Kenya for example, text messages, blogs and radio had already been found to have played a role in the post-election violence of the 2007/2008 elections.[16] The 2013 Kenya election was also rife with divisive and inflammatory content on social media, where it found an outlet following tighter controls on print media and telecommunications.[17]

Online space is a magnet for all come election time. Political campaigning has always been a messy affair and while data driven political campaigns are not new, the granularity of data available and the potential power to sway or suppress voters through that data is, particularly through targeted political advertising online.

5 • Targeted Political Advertising Based on Data Analytics

Political campaigns around the world have quickly turned into sophisticated data operations. The way in which data is used in elections and political campaigns is potentially highly privacy invasive, raises important security questions, and has the potential to undermine faith in the democratic process.

Social media platforms make money from targeted advertising, based on the user information they collect, including demographic information, location and detailed interests.[18] In the same way that online advertising targets people based on interests, personality and mood to ultimately sell products, political parties persuade you to buy what they are selling come election time.

In short, this means that companies, many of which you have probably never heard of, are able to learn about your habits, personality, sexual interests, political beliefs and more to make predictions about your personality and behaviour. This is known as "profiling".[19] Profiling generates highly sensitive inferences and predictions about people's personality, behaviour and beliefs. Voters are ultimately being profiled based on information they did not necessarily know they had given up. This is especially concerning when sensitive information, such as political beliefs or personality traits are inferred from completely unrelated data using profiling.

Political parties contesting elections directly employ data analytics and digital media firms, who are adept at profiling, to run their online campaigns. These firms, in turn, may work directly with online platforms, like Facebook, to craft micro-targeted political messages that are designed to influence the way you vote, based on information collected and inferred about you. They frequently rely on commercially available data from data brokers, or publicly available records and data that is accessible online to build highly intimate profiles, including conclusions about your personality, fears and emotional state. Targeted campaign messages and adverts can then flood online search results and social media feeds. The 2016 Trump presidential campaign, for example, used up to 40-50,000 variants of the same online messages every day in order to target different groups of people.[20] But the details behind this process are often unclear – exactly who these companies work for, what they do, how they do it, what data they collect and how successful they are, are all closely guarded secrets.

In early 2017, Privacy International investigated a report that the United Kingdom (UK) based data analytics company Cambridge Analytica was discreetly working for the ruling Jubilee Party in the run up to the Kenyan presidential elections. We wrote to the company in May 2017 to ask for clarification on its role and how, as a British company, it was adhering to data protection laws when Kenya has none.[21] We were concerned that the potential data gathering could be extremely intrusive, including sensitive personal data such as a person's ethnicity. In countries where there is history of ethnic tensions resulting in political violence, such as Kenya, campaigning based on data analytics and profiling is untested ground, fraught with great risk. We received no response.

Our sources confirmed that Cambridge Analytica was indeed working for the Jubilee Party, gathering survey data to aid the campaign and managing the image of the President. Around the same time, two inflammatory online campaigns, The Real Raila and Uhuru For Us, targeting the Kenyan opposition began circulating online in Kenya. Their creation was claimed by "a group of diverse and concerned young Kenyans", and played heavily on Kenya's violent past elections and fears of any future violence. The Real Raila campaign claimed that opposition candidate Raila Odinga's administration would "remove whole tribes".[22] As these videos dominated Google searches and flooded Twitter, Facebook and YouTube accounts across the country during 2017, Privacy International conducted an in depth investigation[23] into the origins of the videos.

As it had already been established that Cambridge Analytica was working for the Jubilee Party, we expected some involvement on the part of the company in the creation of the videos. However, Privacy International's investigation revealed that Harris Media LLC created the videos, a Texas based agency that uses data analytics to create political campaigns. On this occasion, targeting was done through judicious use of Google AdWords, where paid-for ads for the campaigns were displayed above Google search results for many Kenyan election-related search terms, such as "Kenyan election date".

However, it was only in March 2018, following the investigations by The Guardian newspaper and Channel 4 News in the UK that Cambridge Analytica was catapulted to the top of the news agenda. A whistleblower came forward describing the "harvesting" of Facebook profiles to target voters during the 2016 US presidential election.[24] A Channel 4 News undercover investigation secretly filmed Cambridge Analytica employees boasting about their involvement in elections, including in Kenya. Mark Turnbull, the Managing Director of Cambridge Analytica Political, a subsidiary of Cambridge Analytica, confirmed this and more in the undercover video,

> *We have rebranded their entire party twice, written their manifesto, done two rounds of 50,000 surveys, huge amount of research, analysis, messaging and then we'd write all the speeches and stage the whole thing, so just about every element of his campaign.*[25]

Further Channel 4 News reporting that focused on Kenya also highlighted the spread of the online videos[26] detailed in our earlier investigation. What remained unanswered however was exactly what kind of data was collected on Kenyan citizens, from what sources and what Cambridge Analytica's specific involvement was. We do not know, for example, what data may have been collected or shared by either Facebook, other platforms, or other data analytics firms working in Kenya during the elections.[27]

However, the scandal spawned a wave of welcome analysis and discussion on corporate behavior and a lack of safeguards for personal data all over Africa.[28] This currently unfolding story is indicative of a powerful and opaque corporate ecosystem behind targeted online political advertising which thrives on our personal data – either to sell us soap or persuade us who to vote for.

6 • Transparency in political campaigning

In countries with a history of political violence, it should not be "business as usual". Ethnicity in Kenya, for example, is still a sensitive issue and elections are a time of heightened tension. Therefore, at the very least, companies in this ecosystem must be transparent about their role in online political campaigns. Kenyan electoral laws do not clearly require candidates to acknowledge campaigns or adverts they have funded. The companies involved are not forthcoming about their role. It is essential for political campaigns to be run in a transparent and accountable way, particularly when the stakes are this high in a country like Kenya. Currently, targeted online political advertising is neither.

It is not controversial to demand that political parties be transparent about the marketing campaigns they have funded, how they have developed targeted messages, or with which companies they have worked. When it is not transparent who has funded or created campaign adverts, there is no accountability.

Healthy democracies are not just about voting. Kenya is only one country where biometric voter registration and authentication exists with challenges, and it will take time to untangle the web of companies exploiting personal data for campaigns paid for by political parties. The difficulty, of course, is that those that benefit are political parties themselves. Why would they change a system that helps them get into power?

Kenyans must wait a few years until the next election. For all those with elections this year, protect it by demanding transparency and proper protections, from registering to casting your vote. It counts, more than ever.

NOTES

1 • "Texas Media Company Hired By Trump Created Kenyan President's Viral 'Anonymous' Attack Campaign Against Rival, New Investigation Reveals," Privacy International, December 15, 2017, accessed June 6, 2018, https://privacyinternational.org/feature/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack

2 • "Biometric Technology, Elections, and Privacy. Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process," CIPIT at Strathmore University, Nairobi, May 2018, accessed June 6, 2018, https://blog.cipit.org/wp-content/uploads/2018/05/Biometrics-Privacy-Report-by-CIPIT.pdf.

3 • "Report of the Independent Review Commission on the General Elections held in Kenya on 27th December, 2007" (known as the Kriegler Commission), Recommendations Concerning Registration of Voters, p. 157, Kenya Law, 2008, accessed June 6, 2018, http://kenyalaw.org/kl/fileadmin/CommissionReports/Report-of-the-Independent-Review-Commission-on-the-General-Elections-held-in-Kenya-on-27th-December-2007.pdf.

4 • *Ibid.*, Annex 3.A, pp. 260-295.

5 • *Ibid.*, p. 8.

6 • Agence France-Presse, "Dead Voters and Other Ways to Steal a Kenyan Election." The Daily Nation, August 1, 2017, accessed June 6, 2018, https://www.nation.co.ke/news/Kenya-General-Election-2017-and-rigging/1056-4040292-5toedlz/index.html.

7 • Dale T. McKinley and the Right To Know campaign, "New Terrains of Privacy in South Africa." Right2Know, December 15, 2016, accessed June 6, 2018, http://www.r2k.org.za/2016/12/15/research-new-terrains-of-privacy-in-south-africa/.

8 • Dhananjay Mahapatra, "Supreme Court Reserves Verdict on Aadhaar Validity." The Times of India, May 11, 2018, accessed June 6, 2018, https://timesofindia.indiatimes.com/india/supreme-court-reserves-verdict-on-aadhaar-validity/articleshow/64116972.cms.

9 • "Biometrics in Kenya's Election," CIPIT blog, 2017, accessed March 27, 2018, http://blog.cipit.org/wp-content/uploads/2017/12/Biometrics_history.png.

10 • Dell Cameron, "Private Records of 93.4 Million Mexican Voters Exposed In Data Breach." The Daily Dot, April 22, 2016, accessed June 6, 2018, http://www.dailydot.com/layer8/amazon-mexican-voting-records/.

11 • Vladimir Hernandez, "Our World: Kidnapped in Mexico." Huffington Post, March 15, 2017, accessed June 6, 2018, http://www.huffingtonpost.com/vladimir-hernandez/our-world-kidnapped-in-mexico_b_9462258.html.

12 • "State of Privacy Report for The Philippines," Privacy International, January 2018, accessed June 6, 2018, https://www.privacyinternational.org/state-privacy/1009/state-privacy-philippines.

13 • "Biometric technology, elections, and privacy," CIPIT, May 2018.

14 • Mike Wendling, "The (Almost) Complete History of 'Fake News." BBC, January 22, 2018, accessed June 6, 2018, http://www.bbc.co.uk/news/blogs-trending-42724320.

15 • Ethan Zuckerman, "The First Twitter Revolution?" Foreign Policy, March 24, 2011, accessed June 6, 2018, http://foreignpolicy.com/2011/01/15/the-first-twitter-revolution-2/; Essam Mansour, "The Role of Social Networking Sites (SNSs) in the January 25th Revolution in Egypt," *Library Review* 61, no. 2 (2012): 128-159.

16 • "On the Brink of the Precipice: A Human Rights Account of Kenya's Post-2007 Election Violence," The Kenyan National Commission on Human Rights, 2003, accessed June 6, 2018, www.knchr.org/Portals/0/Reports/KNCHR_REPORT_ON_THE_BRINK_OF_THE_PRECIPE.pdf.

17 • "Corporate Responses to Hate Speech in the 2013 Kenya Presidential Elections. Case Study:

Safaricom," The Institute for Human Rights and Business, p. 23, November 2013, accessed June 6, 2018, https://www.ihrb.org/pdf/DD-Safaricom-Case-Study.pdf.

18 • For example, Facebook Business, Homepage, 2018, accessed June 6, 2018, https://en-gb.facebook.com/business/products/ads/ad-targeting.

19 • Profiling is a term outlined in the forthcoming European General Data Protection Regulation (GDPR). It is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements". "Article 4 EU GDPR 'Definitions'," Privacy Plan, 2018, accessed June 6, 2018, http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm.

20 • Sean Illing, "Cambridge Analytica, The Shady Data Firm that Might be a Key Trump-Russia Link, Explained." Vox, March 17, 2018, accessed June 6, 2018, https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-christopher-wylie-facebook-trump-russia.

21 • "Letter to Cambridge Analytica on 2017 Kenya Election," Privacy International, May 30, 2017, accessed June 6, 2018, https://privacyinternational.org/advocacy-briefing/1683/letter-cambridge-analytica-2017-kenya-election.

22 • "Kenya in 2020 if Raila Odinga is elected President," YouTube video, 1:28, posted by The Real Raila, July 10, 2017, accessed June 6, 2018, https://www.youtube.com/watch?v=o45NlqZXDXw.

23 • "Texas Media Company Hired By Trump...," Privacy International, 2017.

24 • "The Cambridge Analytica Files," The Guardian, March 2018, accessed June 6, 2018, https://www.theguardian.com/news/series/cambridge-analytica-files.

25 • "Revealed: Trump's Election Consultants Filmed Saying They Use Bribes and Sex Workers to Entrap Politicians," Channel 4 News, at 9", March 19, 2018, accessed June 6, 2018, https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation.

26 • "Kenyans Bombarded With Fake News in Presidential Election," Channel 4 News, March 25, 2018, accessed June 6, 2018, https://www.channel4.com/news/kenyans-bombarded-with-fake-news-in-presidential-election.

27 • "Further Questions on Cambridge Analytica's Involvement in the 2017 Kenyan Elections and Privacy International's Investigations," Privacy International, March 27, 2018, accessed June 6, 2018, https://medium.com/@privacyint/further-questions-on-cambridge-analyticas-involvement-in-the-2017-kenyan-elections-and-privacy-15e54d0e4d7b.

28 • Maggie Fick and Alexis Akwagyiram, "In Africa, Scant Data Protection Leaves Internet Users Exposed." Reuters, April 4, 2018, accessed June 6, 2018, https://www.reuters.com/article/us-facebook-africa/in-africa-scant-data-protection-leaves-internet-users-exposed-idUSKCN1HB1SZ; Nick Miriello, David Gilbert and Julia Steers, "Kenyans Face a Fake News Epidemic." Vice, March 22, 2018, accessed June 6, 2018, https://news.vice.com/en_us/article/43bdpm/kenyans-face-a-fake-news-epidemic-they-want-to-know-just-how-much-cambridge-analytica-and-facebook-are-to-blame?utm_campaign=sharebutton; "Kenyans Want to Know What Role Cambridge Analytica Played in their 2017 Presidential Election," Vice News, March 22, 2018, accessed June 6, 2018, https://www.youtube.com/watch?v=0xw-DhxNv2Q.

LUCY PURDON – *United Kingdom*
Lucy is a Policy Officer with Privacy International and is responsible for policy development. She leads the global policy work on cybersecurity and identity. She works across the organisation and with international partners to develop policy recommendations and positions based on research project findings.

email: *lucyp@privacyinternational.org*

Received in March 2018.
Original in English.