At the start of summer 2020, Tactical Tech's Data and Politics team collaborated with political analyst and writer, Nanjala Nyabola, to hold a virtual round-table to discuss the trends in the use of personal data in political campaigning in Sub-Saharan Africa. The two-day discussion addressed questions such as what data-driven campaigning methods are employed by political parties and groups in the region; who is involved in the collection, analysis and use of personal data; and what short and long term impact does data-driven campaigning have on political participation.

The aims of the round-table were threefold:

- To provide groups and individuals from civil society with a foundational understanding of the influence industry and a framework for analysing data-driven methods used in political campaigning
- To build an overview of the methods currently being employed in the region, by which actors, and to begin to build a community to continue building this knowledge together
- To analyse the challenges that data-driven political campaigning may be creating for political participation in the region, in order to inform explorations into practical solutions

The round-table was attended by researchers, lawyers, communication professionals, policy-makers, campaigners, and educators with backgrounds in technology, political science, data protection, and elections. The attendees were based in Uganda, Nigeria, Kenya, The Gambia, Zimbabwe, Togo, Ghana, Canada, UK and Germany. Some of the attendees work locally, and others work across several countries in the region.
The topics discussed included analogue data collection, the catch-all justification of ‘national security’ for sharing data, fake news pedlars, the exporting of data-driven methods by French or North American companies, the use of billboards outweighing the use of personalised tactics, the digital divide leading to an exclusion from politics, and more. The conversation was nuanced and productive, discussing shared readings, personal experiences of data-driven practices, methods of research and ideas for the future. Read on to find out more.

Note: Names of attendees have not been included, apart from speakers, to ensure anonymity, but this report is the product of all attendees’ shared knowledge. Some of the commentary is the result of the attendees’ research, some from their experiences, and some speculative. References are included where possible. If you would like to find out more please feel free to get in touch with the Data and Politics team at Tactical Tech.

Contents:

- Introducing The Influence Industry, Varoon Bashyakarla (Presentation)
- Data-driven Politics in Sub-Saharan Africa, Nanjala Nyabola (Presentation)
- Commentary on Past Research, All (Discussion)
- Data as an Asset, Influence, and Intelligence, All (Discussion)
- Feminist Approach and Ordinary Voices, Nanjala Nyabola (Presentation)
- Research Using WhatsApp, Jamie Hitchen (Presentation)
- The Research Questions, All (Discussion)
- The Research Challenges and Solutions, All (Discussion)
- The Consequences of Data-Intensive Politics, All (Discussion)
- Long and Short Term Solutions, All (Discussion)
- Final Remarks, All (Discussion)
- Appendix
Introducing The Influence Industry, Varoon Bashyakarla, Tactical Tech (Presentation)

The majority of discussions surrounding the use of personal data in political elections has focused on three areas: Facebook, disinformation, and the US (see image 1). Tactical Tech has chosen to focus their research beyond each of those. Firstly, Tactical Tech has researched the companies beyond Facebook, the industry of more than 300 other companies involved, including data brokers, digital campaigning consultants and advertising firms who are involved in data-driven political campaigning. Secondly, Tactical Tech is examining the ‘legitimate’ data-driven communication practices, software and companies used in political campaigns, without concern for whether the aims were nefarious, such as maliciously producing misinformation. Finally, Tactical Tech has conducted research with partners across the world to examine similarities and differences in practices across different countries and different regions.

Image 1: A Venn diagram showing where the data and elections discussion has focused so far. Tactical Tech has placed their research to go beyond each of those, to the companies beyond Facebook, the pervasive practices that are considered legitimate, and a global approach.

During this research two big questions keep coming up that Tactical Tech have also been keen to move away from: Does it work? and What’s the next big scandal? It is really important that we go beyond these questions to examine the methods that are increasingly common practice without scandal, whether they have effects on final votes or not, as the processes and practices themselves shape the type of politics we participate in. Tactical Tech’s Data and Politics team undertook research to address these wider

1 https://ourdataourselves.tacticaltech.org/posts/whos-working-for-vote/
2 https://ourdataourselves.tacticaltech.org/chapters/dap-ii-methods/
3 https://ourdataourselves.tacticaltech.org/chapters/dap-ii-country-studies/
questions over two years of work with 15 local partners across the world. While this work is ongoing in 2020, the research up to this point was published in a report, Personal Data: Political Persuasion: how it works, and a virtual gallery of the 300 companies (See image 2).

Image 2: Quilt of companies that work on the topic, demonstrating the influence industry that goes far beyond Facebook

Data-driven Politics in Sub-Saharan Africa – A contextualisation, Nanjala Nyabola (Presentation)

The current context of a global health pandemic shows more than ever why we need to focus on who is voted in, because a public health emergency requires leadership that you want and who knows what they are doing. It is also really important to address this topic with an understanding of the way Western-developed technologies are used in African contexts, from high tech surveillance to data-driven communication tactics.

Data has become a massive market opportunity in participatory politics and in elections in the last 10 to 15 years. Countries in the region, such as Kenya, have an electronic voting system. However, it is not just the process of voting, but the campaigns around the elections that are reliant on data-driven technologies. Furthermore, a lot of governments are moving to digital public service provision. In Kenya, this includes an exercise leading to a ‘single source of truth’ identity system. This is called The National Integrated Identity Management System (NIIMS) that would connect people’s national ID to their biometrics, land registry department records, school records and other personal information held by various government bodies. This system has yet to be fully implemented, as a debate

4 https://ourdataourselves.tacticaltech.org/posts/inside-the-influence-industry/
currently continues as to whether this system will go ahead as there are many unresolved issues. The High Court of Kenya, for example, has ruled that there would first need to be a data protection law in place.\(^6\)

When governments collect massive amounts of public information to regulate society, there are always political consequences to be interrogated. This is especially true without a legal framework. The framework should take into account issues that have been proven to be problematic in these systems including the effects of disproportionate resources and discriminations in-built into the technology systems. For example, there are vast amounts of people in Kenya without birth certificates, and the systems don’t have space for those discrepancies.

Another centralised database of personal information in Kenya is the Integrated Financial Management Information System (IFMIS). This system was built in order to address issues of corruption. However, this system has created black box in government in which a person working on the system can siphon money off without accountability as there only marginal opportunity for scrutiny. There is no transparency about how the system is administered or how data is collected or accounted for, and it is difficult to track. Within the country's IT infrastructure, it is possible to connect tax and bank details, but there is, again, no legal framework to protect the data, no interrogation into what the data is being collected for, and no way for the citizens to claim accountability. The tax service already connects to banking services. While this is, in theory, for a good reason to easily pay tax, the technology systems, processes and tools have vulnerabilities which put data at risk.

Big mobile companies are another component of the personal data system in Kenya. Safaricom, for example, is a government-owned communications utility, and they gather personal data for ‘tax’ purposes and ‘government’ purposes. This places the government’s hand on the scale and gives them disproportionate ability to affect the conduct of communication utilities. (The use of mobile networks for political campaigning are further discussed in this report).

One of the challenges that has emerged in Kenya, and to a lesser extent Uganda, is that there is a lot of information being gathered but there is not a lot of change or impact on public services based on this data collection. For example, government petitions are carried out, which, if they hit a set amount of signatures, must be discussed by government. However, the government say ‘you’ve got two days’ to write your memo about whatever the topic is, and dismiss the results. The speed and immediacy of digital is making it easier to dismiss the views of the public, and to shut people out of decision making.

Further, there is a feedback loop in which the information which goes into public opinion affects the quality of public participation. If political systems work well, like the data commission, then that feeds into the electoral context: people are voting openly and it

---

reflects what they want. However, people have been consuming so much information that even when they come to vote it can be difficult for them or observers to know what information they have seen, and which of that information has influenced their decision; even an open vote can not reflect a public vote. The systems we are building are complicated and not fit for purpose, and we need to find points in the feedback loop to break the cycle.

A summary of the key threats are

- unchecked data collection
- monetisation of personal information - I give my data to the electoral boundaries commission to take part in the electoral system and they sell that to a broker, maybe in France, who are building propriety software for elections, that is against my best interests
- surveillance
- privacy
- consent to be governed
- discrimination and historical injustices - many countries here have communities that have been denied the right to legal identity and these digital structures compound those issues
- lack of transparency in political decision making
- corporate influence on political outcomes - Cambridge Analytica does not have to deal with the outcomes of the election, and the government elected in. This is a form of colonialism, and I really want people to think critically beyond the technical aspects to what are we seeing in the balance of power between Canadian, French, and Australian companies, and the political context in Africa.

The following issues are to be considered when thinking about political influence, which all affect the balance between political parties, companies and on the other hand citizens (not users, or customers - but citizens who have very little power):

1) a bombardment of information making it difficult to understand what information to take in
2) messing around with the political agenda to hide the important issues
3) preference shaping: hiding certain things from media and public knowledge.

A few more problems to be considered in the discussion: money matters when it comes to voter data. Specifically, in elections this money is for party memberships and voter
identity information, including social and traditional media showing voters’ preferences and opinions.

There are also patterns around the release of election results. For example, there are often internet shut downs around waiting for results.

There is also an issue around civic tech and activism, and how civil society groups are provided with tools that are owned by private firms, and ultimately contribute to the shrinking space that surrounds where civil society can take place.

Finally, we need to pay attention to all the key actors: the citizen and the state, corporations, public institutions, the judiciary and civil society. We need to work out how to put more tools in the hands of citizens so they can understand what is happening. The judiciary is a separate actor too, as during proceedings around the elections it was clear that lawyers often do not have knowledge of the technical aspects of how the influence economy works.

The key questions to consider are:

- How do we protect citizen data created by electoral processes from undue corporate influence?
- How do we protect the sanctity of the institutions that are supposed to be custodians of citizen data?
- How can we use data to restore the balance of power between the citizen, the state, and private corporations in African elections?

The positive in all of this is that people are feeling increasingly empowered to do something about it. This frames the productive sides of the conversations and the solutions we can discuss. (Some of these are presented in this report.)

Commentary on past research, All Participants (Discussion)

The following two reports were used as a starting point of the discussions. This section captures a few of the main comments from participants on these pieces.

Personal Data and Political Persuasion: Inside the Influence Industry

Track, Capture, Kill: Inside communications Surveillance and Counterterrorism in Kenya

Observations and commentary on the literature (see also image 3):

- One of the major complaints about the government collecting personal data is that they are not ICT ready, but it is clear from report that the government can have access to, and use, very sophisticated digital tools.
It is useful to read what happens once a phone is taken from someone, or to the data once it is collected, for example when this is then passed on to a central database or shared with other firms.

There is a difference between intelligence - based on data collected and analysed - and a genuine understanding of constituents.

Many private firms based in and associated with other countries, such as Cambridge Analytica, have worked with political parties to conduct profiling and online messaging in Kenya.

The same intelligence technologies are used in security and in politics.

It would be useful to know how countries in Africa learn from each other, for example, how The Gambia will learn from the practices in Kenya and elsewhere.

Technology used in campaigning has changed from 2015 to now, and there are still technologies being used or developing that we don't know of yet.

National security is used to defend the government’s collection of data from agencies such as telephone network companies.

It is notable that a lot of techniques are tested in African and Asian countries rather than 'coming from the West'.

There are fewer attempts to connect voter data to campaigns than expected, for example, in Nigeria they were not using the data collected in the app but giving cash to communities or other persuasive techniques instead.

Nigeria have just introduced a smart card to vote which is connected to their driver's license and/or other identification methods.

It is useful to evaluate how data is used with different values: for asset, influence, or intelligence.

In Senegal in 2018/19 they used surveys and in Gambia they are planning to do this.

The results of surveys are used to win over swing voters or target opposition voters.
**Data as an Asset, Influence, and Intelligence, All (Discussion)**

Beyond micro-targeting, there are various uses of data used in data-driven campaigning. Tactical Tech have categorised these into three types of use: data as an asset, data as intelligence, and data as influence. These are described in this section, along with a discussion on what specific methods and tools are used within these categories in Sub-Saharan Africa.

**Data as an asset**

Data on voters is valuable in itself: private companies boast about the quantity and variety of data on voters that they can gather and share with political parties; there are private and public trades of data; political parties hold their own databases, usually filled in by electoral rolls which are released by governments, containing at least the name and address of everyone who can vote; and there are attempts to open up access to the valuable data through leaks, breaches and hacks of these databases.

In discussion it was reported that in Kenya, the electoral roll – the list of eligible voters, their addresses, and subsequently the region they will vote in – is accessible to political parties. The political parties then often share this database with the corporations they work with, such as digital campaigning firms they hire. Another main source of data in Kenya is mobile transferred money which is used both between individuals and to buy products in cafes or shops. The companies involved, such as M-Pesa, collect names, contact details, and financial records. These records can be shared with private firms or government bodies on request. Another source is paper sign-in sheets used for people to sign into buildings, supermarkets and pharmacies which companies can go round to collect. It is clear if you search for your name, that your information will have been collected from one of these sheets and you may even have been signed up to a political party that you have not even heard of. In Kenya, betting companies have also suffered from data leaks⁷, and the majority of owners of these companies are also politicians. The same data actors span public and private spaces. There are breaches of data from gamblers.

Participants drew similarities between Uganda and Kenya. In Uganda, the operations are not visible, and data is collected through voter registration and secondary sources, such as telecommunication companies, which can collect data as it is mandated by law for counter-terrorism. In 2012, in Uganda different arms of the government had different sources of data on people and the government consolidated this through the national ID scheme. This includes biometric data. This data is accessed by political parties. In at least one political party, they have a data scientist who has troves of granular data including financial and geo-location. There is also growing evidence of the government’s presence / "muscle" in the private sector. In the past decade, the government has acquired different intelligence tools all over the world for counterterrorism purposes.

---

In Nigeria and Ghana the electoral register is maintained by the election monitoring body and the basic data is free to access. There are also bespoke polls carried out by private firms on behalf of political clients. In 2017, a company in Uganda, Eskimi, allegedly had the most (granular) data on markets in Uganda and Nigeria. This is an equivalent of DoubleClick, Google’s advertising management system. The development of these companies suggest that things like geofencing will be more common in the future. It is mandatory in Nigeria to have a mobile number registered, and your location shows from your mobile, and it shows if you are voting in one location and studying in another. Data can be legally accessed through Nigeria’s Independent National Electoral Commission (INEC), but mobile phone companies have much more data than the INEC. 80 million people are registered in INEC’s electoral register. This might explain the lack of uproar over privacy breaches. In Nigeria there is NOA, a polling agency which connects with 5 million people and centralises and combines data from INEC and mobile phone data.

In Zimbabwe, data is also collected from money transfer systems and mobile networks, the largest of which are part of the same telecommunications group, and are called EcoCash and EcoNet respectively. In Togo and the Ivory Coast, spyware called Pegasus has been found. In Senegal, data driven campaigning is only just starting.

Overall, many of the techniques described for each country, other people agreed could be employed in the country or region in which they are based, too. It is noted most of the data is likely to have been collected illegally. There is very little canvassing door-to-door to gather data, in contrast to Europe. There are also lots of avenues for data leaks. Not everyone on the lists of collected data are voters, but they are treated as if they are. It is not too difficult to buy national health and insurance data. It is noted that these issues don’t just affect voters and elections, but civil society and people who attend protests.

**Data as Influence**

Data is used to target voters with the aim of influencing their opinions and behaviours. This includes methods such as geo-fencing to target your message only to people in certain postcodes. Another method is search influence, such as finding paid and unpaid ways to change the reach of your content on search engines. For example, when searching the word “scandal,” perhaps to find the TV show, a website of a negative campaign against Kenyan presidential candidate, Raila Odinga, is the top search result (see Image 4). Robocalls, online advertising spaces, texts, and emails are other common methods in which data is used to influence people.
One of the most common methods discussed was bulk SMS. For example, a senator in Kenya messages the people in his district to share what projects he is working on. It is not clear where he would have got the numbers from. These messages can appear very personal, and are very effective in making people feel involved in politics, and connected to the political candidate who messages. This same feeling of an effective personal touch is also true for robocalls, which has also made them very effective. The mobile networks mentioned above who have access to vast amounts of data, also help send out these text messages and calls.

People who use Safaricom in Kenya, which has around 63% of the market share, get more political messages than anyone else. The current ruling party created a message from the president (“Fellow Kenyan, I appreciate your support, let’s work together…”). People receive these robo-calls and get excited that Uhuru contacted them personally and then get excited about the Jubilee party.

In Ghana and Nigeria, often targets of any ‘influence’ tactic are swing voters. They are targeted not just through texts or other digital methods discussed, but also rallies and other traditional campaign activities. Ghana only needs a very small margin of victory in elections and are preoccupied on targeting swing voters by any means.
In Nigeria, there has been a use of robocalls and mass SMS. Empirical evidence from Nigeria suggests that political actors tend to target partisans, not swing voters. However, the centre of democracy and development's research on digital advertisers suggest that robocalls and bulk SMSs specifically may target swing voters. In Nigeria there is also a new rule preventing bulk SMSs from being sent to help protect people's data. Email is not effective (people are not going to read it), but people are much more likely to read their texts. There are also Telegram groups (a few thousand participants) and WhatsApp groups of 256 people. There are also modified or knock off versions of WhatsApp to reach more people.

In Zimbabwe, over 10 million people in 2018 woke up one morning just before the election, finding an SMS on their phones asking them to support a candidate for president despite having never given their phone numbers to the party. There was a long back and forth of finger pointing about how this came about, and whether it should have but it has not been very conclusive. It is suspected of the Telecom company sharing the numbers.

A few technologies are used in Uganda. In 2011 elections, robocalls were used. In 2015, bulk texting and spamming from the president and opposition.

On WhatsApp, one of the consultants claimed to have used undisclosed software, on the eve of the election, to send WhatsApp messages posing as his client's competition. The message said that the opposition candidate had stepped down- his client won that election.

**Data as Intelligence**

Political intelligence techniques are not techniques that land in front of a voter, but rather are used to learn about the voter. There is often a conflation of micro-targeting (influence) and learning and analysis (intelligence). One of the major techniques used in intelligence is A/B testing, and another is the use of website analytics programs such as Google analytics. Public polls and digital listening are also conducted to learn about public opinion.

There is much less understanding of how data collected is used as intelligence or what knowledge is created from the data.

In Nigeria, one consultant claimed to have known the results of voters' actual votes from a past election based on 2015 - and claims to know from that there the most active demographics were fisherman, students, and farmers. Also in Nigeria, its about getting your supports to turnout and reducing those likely to turn out for your opponent.

---

8 https://www.semanticscholar.org/paper/Clientelism-and-Party-Politics%3A-Evidence-from-Zovighian/8e0cd0db8a450f0bf1ad55a7ea356758f57c5e9e
9 https://www.cddwestafrica.org/
In Ghana and Nigeria, swing voters are targeted. Though it is not noted how they are decided or analysed to be swing voters, there must be some analytics done through polling, predictive analytics or past voting records to understand who would be a swing voter.

In Uganda, bulk texting and robocalls have been used as a source of intelligence - again, there is an understanding that the results of who they reach may be taken into account but exactly how or what it feeds into remains hidden from public scrutiny.

**How do we find out more? Research questions, methods, and challenges**

**Feminist approach and ordinary voices, Nanjala Nyabola (Presentation)**

I did not start out wanting to write about technology in politics; instead I started at the point of political science and feminism: it was about understanding these ordinary groups that don't have that specific look of the men in power.

I use mixed methods. I tend to use quantitative methods, but data on the internet is expensive. I combine this with life histories of powerful and not powerful people. It was important to talk to these groups about their lives in a qualitative form as you see what you wouldn't see ordinarily. I have used the women's rights movement as an entry point into how discussions in social media are influencing offline behaviour: the amplification effect. Being comfortable in quantitative and qualitative is really important in this topic, as it's not just a linear track of 'online activity' to 'offline action'.

It is also part of the feminist methodology to use stories and life histories when conducting research. Research on African politics definitely has a power bias, and there is an instinct only to look at things when they effect powerful people - people always want to focus on big stories. There is so much research now into the digital campaigning firm Cambridge Analytica or the data broker Aristotle, but there is little interest in Africa and the contexts away from power. However, there are a lot of things of interest happening across the region.

The dominant tools used for research, such as Facebook, are not very helpful because they are not used in the same way in African society as the creators imagined them being used, or the way the Western researchers use the tools themselves. For example, the free internet generated by Facebook can really affect how people are using it, as it helps the companies advance their agenda, and it's important to keep a cognitive difference between how Facebook is being used and why it is being used like that.

**Research using WhatsApp, Jamie Hitchen (Presentation)**

WhatsApp granted one million dollars to organisations to look at how WhatsApp was being used to spread misinformation after concerns about its use in elections and inciting violence made the headlines in India and Brazil. WhatsApp had no say in what could or

12 https://www.whatsapp.com/research/awards/announcement/
should be published from the research, or how the researcher’s did the research, just that it was done. out of the 20 grants, only one focused on an African country (Nigeria): it is difficult to find money to do research in the region.

There is often an argument that there is little impact of internet driven technologies due to low internet penetration, but this is not true. In Sierra Leone, there is only around 4% of people using WhatsApp, but the impact can reach further than those 4% both now by a ripple affect to the contacts of those 4%, because social media content shapes and informs wider media content and because those 4% are often some of the most influential people in society.

Our research in Sierra Leone and Nigeria was to examine WhatsApp which has its own difficulties because it is not a public platform. It is difficult to get quantitative data on the usage, because it is unavailable, and it might not be useful even if you could have it due to the volume of messages shared each day. I currently have 947 messages in the Sierra Leone group alone from one day. Users can only see what groups they are in share, and there are also ethical questions about joining groups for the purpose of researching what they are discussing; as WhatsApp is a private messenger application and so listening in to conversations without having group member approval is akin to spying.

Our approach was to conduct interviews and surveys with users, particularly those engaged with electoral politics, to see how people are using the tool. We also conducted survey work in Nigeria to see what kind of information was shared and what form it took. This allowed us to get a sense of what gets inputted to WhatsApp, and what users get out of it, without infringing on their privacy. Context is critical, and thus working in partnership with Nigerian-based research institution CDD was key to helping situate the discussions in the political reality. This also ensures audio, video and picture content, some of which is deliberately misleading, and which is often not in English, can be included in the analysis.

One thing we haven’t done a huge amount of, but has been done in India, is sitting with an individual as they use the platform and asking them questions while they are doing it. It’s a more ethnographic approach to understand how information flows.

**The Research Questions, All (Discussion)**

Building from the discussions on day 1 and the morning of day 2, the following research questions arose:

How much cross-country learning is going on within Africa? Is it the case, for example, that Gambian political parties are learning from, and adapting approaches employed in Senegal or even places further away like Malawi or Kenya?
Which groups are most likely to receive data-driven communications and for what aim? More specifically, is data used to sway swing voters or target voters for the opposition?

There is obviously a lot of variance in the degree to which data is used in different elections, by different parties, in different countries. What factors explain this?

What could be done to ensure transparency and accountability of the use of personal data in elections? What is preventing it from happening?

What do voters need in order for their data to be protected? Especially when Covid-19 stops large crowd gatherings?

Is there a clash of values if voter data needs to be protected but electoral law requires the electoral commission to release lists of voters to political parties ahead of the polls?

Is the data actually used after being collected? What factors stop data being used (e.g. lack of perceived effectiveness, or lack of resource)?

Traditional methods are still largely used, such as billboards and rallies: what factors are present when traditional methods are used and what factors influence when data-driven methods are? Is personal data influencing when and how the traditional methods are, used such as in Togo or Guinea?

Fake news pedlars are proud of their work, and often boast their abilities to political campaigns: what effect are they having?

How can we employ data-driven research methodologies and tools to investigate personal data abuse during/around election times -- as opposed to months before or after elections?

Can data protection ever go 'backwards' or are we bound to the progress of technology and increasingly present data-driven systems?

What can ordinary people do to protect themselves and what needs to be done by other stakeholders?

We are seeing an increasing number of polls/opinion surveys being conducted by media, political parties (or their affiliated consultants) using mobile phones but how are they being used by political parties/candidates (to win over new voters, to target areas to attack credibility of polls/election commissions to reduce turnout, to boost their own turnout) and through/on what digital platforms?
Is the collected data driving the development of election strategies? Or simply a tick-box exercise that needs to be done?

Who else needs access to the information regarding data and politics and where do they look for information? Specifically how can this project be more relevant or visible to different actors pursuing public interest cases around data and politics?

What actors are under-researched, or may be completely unknown to us, and have an effect on the use of personal data in a political participation context? In particular across activism and civil society?

Why do communication companies need to resist sharing data with government bodies? Is it legal or cultural?

What is needed to balance the effects of Facebook being the cheapest way to communicate? Citizens have limited power and resources to address these topics.

In Uganda, even if data is accessible that could hold officials accountable, people are not aware of it. What are the questions we have to ask to engage citizens?

How can institutions/organizations empower citizens? Citizen journalism? Electoral oversight?

The Research Challenges and Solutions, All (Discussion)

There are various methods identified as useful for researching the area. It is important to take a mixed methods approach. There was also a suggestion of monitoring local radio stations. From messaging on radio, to the specific languages in specific regions, you can tell that they are personalising messages to these regions. We need to ask people directly what kind of messages people have seen and how it has affected them, through interviews, surveys, journals or observation. Regional election commissions could be a more formalised way to investigate digital campaigns. We need a constant dialogue between different sectors and groups in our (global) society - cross disciplinary research needs to take place. There need to be tools to help trace hash tags and which social media accounts are pushing certain messaging. Regional and local institutions and groups should be examined. We also need to take a feminist approach to asking new questions. Traditional metrics are not suitable in many contexts, and this is where qualitative and mixed methods could play a part. Investigations need to extend beyond looking at big players, and on big players we need to dig deep.
Resources affect the difficulties in conducting research in several ways. Purchasing data is expensive, controlled by the platforms, and may not have been collected with consent - this is something researchers have to consider as well. It's always the global south being monitored by the global north and it is important to change that dynamic. Data is expensive - it can cost 1,000 dollars to buy a life-cycle of a hashtag. Researching a closed technology is very difficult. Access to hard data is difficult / data is not always as useful as it might be. Platform metrics can't work well in many African contexts and understanding usage needs to understand coded iterations (language). For western researchers, how do we make sure we work with local groups and people to understand what is happening locally, which is necessary for understanding technology. This is also important because there is little money in this space for research and when there is, western researchers are more likely to gain this funding.

Data on political parties is difficult to attain because they do not need to be transparent, and are not. Data consultants are very guarded in the run up to elections. Publicizing their work takes place afterwards. A major issue is that the people who could be good researchers are often employed by political parties. People who start digital rights work often then get hired by digital companies. Then their expertise and knowledge has gone from public knowledge to private knowledge. Any Big Tech research into the topic could be a PR move first and foremost.

The information environment is affected by fake news pedlars who push forward their agendas and opportunities. They are often proud, which may make it easier to ask them directly about their tactics.

There is also a problem with what to do with the research - what impact can it have and is it trying to have. For example, there is apathy towards challenging social media companies. Facebook is still growing, though we know about how it is exploiting our data. These companies are also facilitating social and public life.

It is difficult to know where money is coming from or spent on - can initiate amendment bills - important to watch when amendments are made and who is involved.

The Consequences of Data-Intensive Politics, All (Discussion)

The issues with the techniques are broader than just their effectiveness. The issues range from unequal resources to values which clash with participatory politics, to physical dangers. Some of the following issues and observations were raised:

There is an illusion that data-driven campaigning does not have impact because of the number of people not on the internet - there is a focus on simple causation, it is causal but it isn't as linear as people think - it could even be things that happen in 5 years after several steps in between.
There are various imbalances in power. There is a reinforcement of biases through data-driven politics. We need to think about how to build capacity for digital literacy (generational elements). The best time to equip voters is before elections. There is a digital divide and voters who are not on digital are treated differently. Small political actors are not able to be competitive. Often only the incumbent can afford the premium package. There is also a skills gap: how do people monitor online elections when parties can hire experts, especially from west, who are better place to hack elections?

Even though it has been happening in Nigeria since 2011, there has been no uproar on privacy, and no report about Cambridge Analytica’s involvement. Nigerian investigation into Cambridge Analytica’s work started in 2015, and there is still no report. There seems to be a lack of awareness of data privacy and privacy breaches. In any region, what happens after Cambridge Analytica leaves?

In Uganda in 2011, there was an internet shutdown during election time. In 2016, there was a mobile money / internet shutdown.

How do we study these phenomena beyond the context of national elections (e.g., at group levels -- Nigerian bar data leak)?

A majority of Nigerians don’t see receiving text messages from politicians as an infringement of their rights.

Big Tech and politics are running too close. The data-driven campaigns are undermining participatory democratic processes because elections are won by data engineers and not political ideas and ideologies. Politics has become a competition of marketing techniques not of ideas.

There is an increase in voter apathy. We need to create more awareness of why it matters, because it is easy to not care. Many people think they have nothing to hide. People are disclosing sensitive information (bank accounts details, etc). Every citizen has responsibility for their own data and to defend freedom of speech.

Data-driven campaigns encourage polarisation.

The owners of the public and private sphere are the same.

Infocalypse: There are vast amounts of information, not all of which is true. More information doesn’t lead to more voter participation/debate - simple slogans are much more effective.

Digital tools can be adapted from election operations to mediate other aspects of life and lived experiences, thereby undermining agency, liberty and autonomy. The tools and practices cross over with surveillance.

Once you’re related to a group, if that group is considered illegal that data could be used to pursue you in detention - especially political parties not getting legal recognition.
What are regulators supposed to do, they can't censor information but they have to set a standard - how can they be consistent?

**Long and short term solutions, All (Discussion)**

The last two sessions covered topics of what solutions are possible to some of the research and impact issues.

- Explore the policy environment. Policy alternatives and policy hackathons in order to engage on topics.

- Make it appealing to corporations and parties to not use these techniques (i.e. it is not profitable or it is not effective).

- Broaden the role of those looking at data in campaigns to go beyond social media and media in general

- Voter awareness efforts, including education on privacy concerns so people know to be cautious (not paranoid). Make laws and rights increasingly understandable. Bridge the gap between politics and technical details and demystify the processes for the wider public.

- Create a better understanding among party members.

- Create materials for activists to better understand their rights.

- Understand the technology even more and make it accessible to political science researchers.

- Strengthen the focus of electoral monitoring bodies on data and breaches: make it part of their tool kit.

- Bridge language barriers between users and service providers.

- Create better ways to report misinformation.

- Deliver protection training and risk management for researchers on these topics.

- Encourage multilingualism to counter biases and more regional representation.

- Use strategic litigation to strengthen existing laws and to ensure existing legal standards are being respected.

- Embrace digital tools but have "sensible" limits and regulations.
Educate communications companies to know they can ask law enforcement to show evidence of why they are collecting data.

Strengthen the parameters of existing legislation and provide Best Practice Guidelines for campaigners and candidates. Regional proposal for codes of conduct and best practices - based on data protection laws and regulations.

Include hiring or purchase of data in the cost of political campaigns.

Conduct long-term research on when and why data is not the most effective strategy.

Create regional connections and networks. Connect lawyers on these topics.

Encourage greater recognition from funders of the need for local researchers and meaningful resources for innovative methodologies.

Emphasize the "so what" questions / consequences.

Develop new lenses and structures on how to think about these topics.

Strengthen the intersections between technology and law.

Final Remarks, All (Discussion)

The group gave a final reflection on the workshop (See image 5). People felt energised to continue working on the topic, and positive about meeting everyone. There was shared knowledge about frameworks, methods and local contexts that participants expressed they benefited from.

Image 5: The reflections from participants at the end of the last day.
Appendix

Resources and references

Nigeria Issues New Data Protection Regulation:

Data and politics blog:
http://www.laibuta.com/blog

Zimbabwe’s first-ever election without Robert Mugabe has turned into a privacy minefield:

Kenya’s Safaricom loses market share for fifth straight quarter:
https://www.reuters.com/article/kenya-safaricom/kenyas-safaricom-loses-market-share-for-fifth-straight-quarter-idUSL8N21K1I2

Driving division? Disinformation and the new media landscape in Nigeria:

How Big Data Swung Senegal’s Vote:
https://mg.co.za/article/2019-09-06-00-how-big-data-swung-senegals-vote/

Telecommunications Ownership and Control (TOSCO). A new dataset on ownership of internet infrastructure in Africa, 2000-2016:

Digital Rights in Africa Report 2019:

Mobile Money Platform Surveillance:
https://pdfs.semanticscholar.org/8a61/26d911b2fd5c7e4a24d1f8160b00579a27d9.pdf

Part 1: Inside Safaricom’s Massive Data Breach on Gamblers Data As They Face More Lawsuits In Europe:
This year the following elections will take place in Africa:

October 2020 - Guinea
October 2020 - Tanzania (General)
October 2020 - Cote d’Ivorie (General)
November 2020 - Burkina Faso (Presidential and Parliamentary)
December 2020 - Egypt (Parliamentary)
December 2020 - Ghana (Presidential + Parliamentary)
December 2020 - Central African Republic (Presidential)
December 2020 - Seychelles (Presidential)
December 2020 - Morocco (General)