THE ENGINE ROOM

Digital ID in Zimbabwe: A case study

https://www.digitalid.theengineroom.org

This report is based on research conducted by The Engine Room, with support from Omidyar Network, Open Society Foundations and Yoti Foundation from October 2018 to December 2019.

Researchers: Chenai Chair and Koliwe Majama
Research design consultant: Sophia Swithern
Writing: Sara Baker, The Engine Room
Review and editing: Zara Rahman, Sivu Siwisa and Laura Guzman, The Engine Room
Translation: Global Voices
Layout design: Salam Shokor

Introduction

In 2019 The Engine Room worked with in-country researchers to explore digital ID systems in five regions. The goal of the project was to better understand the true effect that digital ID systems have on the local populations that operate within them.

Our research in Zimbabwe consisted of seven in-depth interviews with key informants in civil society, government offices and the private sector, as well as six focus group discussions with diverse groups, such as farmworkers, a residents' association and a transgender rights group. This primary research was conducted between March and April 2019. All quotations from target populations come from in-person interviews and discussions during this period in Zimbabwe. More information on the methodology can be found in the global report.[1]

With the country's plans for a national digital ID system tied to national security still underway, we expanded the scope of our research to also include the biometric voter registration (BVR) system. Focus groups involved questions about BVR as well as scenario-based discussions, where participants were presented with scenarios focusing on the surveillance aspects of digital ID and then asked a series of questions about their thoughts on privacy.

This project aims to understand the lived experiences of individuals, not to reflect representative samples of each population. We cannot necessarily extrapolate one person's experience to the norm – though there are times when every person interviewed experienced an aspect of a system the same way – but each experience gives us insight into how a diverse range of people is impacted by digital infrastructure and protocols.

The digital ID systems

Through this work, we explored people's experiences with the biometric voter registration system, including the transition from traditional IDs to plastic cards with biometric data, and their thoughts on the national digital ID system.

Leading up to the 2018 elections, the Zimbabwean government introduced biometric voter registration (BVR) in an attempt to solve administrative problems for elections, including voter duplication and ghost voters. This development was accompanied by the need to transition from the old metal ID cards to new plastic cards with biometric data.[2]

The system was fraught with problems from the beginning, as the government outsourced work to companies outside of Zimbabwe. First, China-based Laxton Group won the contract to create

---

[1] See The Engine Room. (2020). Understanding the lived effects of digital ID: A multi-country report.
[2] Share, F. (2017, August 30). RG's office rolls out mobile registration nationwide. *The Herald.* https://www.herald.co.zw/rgs-office-rolls-out-mobile-reg%e2%80%a2-nationwide-programme-to-run-for-3-months-%e2%80%a2-metal-ids-to-be-phased-out/

BVR kits for registration, a move that the opposing party criticised,[3] and then the Zimbabwe Electoral Commission (ZEC) awarded the contract for de-duplication hardware and software to IPSIDY Inc in the United States, a decision that Laxton Group unsuccessfully appealed, claiming it would cause problems in voter registration.[4] In fact, news reports show that the voters' roll later contained 250,000 ghost voters.[5] Other problems plagued BVR. Members of the ruling party convinced some people that BVR could determine how they would vote,[6] and even the ZEC database was hacked.[7]

At the same time, Zimbabwe's Ministry of Labour and Social Welfare was piloting a digital ID system for cash transfers with the help of the World Food Programme (WFP) and United Nations Children's Fund in Rushinga District. Based on WFP's SCOPE, the pilot enabled the government to see how a digital ID system tied to benefits could play out. We were told that the government has not yet approved the use of biometric data in this project, however, limiting pilot findings to the effects of non-biometric digital ID.

Finally, in 2018 Zimbabwe entered into a partnership with CloudWalk Technology, a Chinese artificial intelligence company, to implement a facial recognition programme and national digital ID system linking data to banking and travel. Meanwhile, CloudWalk Technology's motivation is clear: obtaining a database of Zimbabwean faces to refine their facial recognition technology.[8] Eventually, the Government of Zimbabwe realised the value of citizen data to China and demanded a better deal, which led Hikvision, yet another Chinese company to make an offer.[9] Notably, a consultant involved in negotiations said, "We were just giving away our data",[10] making it clear that while Zimbabweans share their data willingly, the government may abuse that trust.

In the meantime, the World Bank has funded a project for the Zimbabwean government to use digital ID to purge ghost workers from civil service, expanding the use of digital ID. In September 2019, several months after our field research ended, the Public Service Commission announced

---

[3] Dube, G. (2017, June 5). Chinese Company Wins $4 Million ZEC Biometric Voter Registration Tender. *VOA Zimbabwe*. https://www.voazimbabwe.com/a/zimbabwe-electoral-commission/3887026.html
[4] Share, F. (2018, January 16). ZEC certifies US firm's BVR tender. *The Herald*. https://www.herald.co.zw/zec-certifies-us-firms-bvr-tender/
[5] Le Roux, J. (2018, July 16). Zimbabwean voters roll haunted by doppelgangers, ghosts https://www.news24.com/Africa/Zimbabwe/zimbabwean-voters-roll-haunted-by-doppelgangers-ghosts-20180716
[6] Majoni, T. (2017, October 23). BVR: The Zanu PF election cheat sheet. *The Standard*. https://www.thestandard.co.zw/2017/10/23/bvr-zanu-pf-election-cheat-sheet/
[7] Mhlanga, B. (2018, July 19). Security breach at Zec, database hacked. *NewsDay Zimbabwe.* https://www.newsday.co.zw/2018/07/security-breach-at-zec-database-hacked/
[8] Hawkins, A. (2018, July 24). Beijing's Big Brother Tech Needs African Faces. *Foreign Policy.* https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/
[9] Prasso, S. (2019, January 10). China's Digital Silk Road Is Looking More Like an Iron Curtain. *BloombergQuint*.https://www.bloombergquint.com/china/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain
[10] Ibid

that they would have all government employees registered in a new biometric system by the end of the month.[11] They plan to commission the verification by early 2020.[12]

Lived experiences

The interviews and focus groups that were conducted in Zimbabwe in March-April 2019 provide insight on the lived experiences of individuals interacting with the described systems. Since there is very little research on people's experiences with digital ID systems, this qualitative data is useful for understanding the reality for some individuals. **It is critical to understand that all residents of Zimbabwe do not have one unified experience. Some of these experiences may contradict official reports.** We aim for these learnings to become part of the broader discussion on digital ID solutions in national contexts.

Awareness and understanding

At the time of writing (November 2019), there remains very little publicly available information about the national digital ID system, and we found no evidence of a large-scale initiative from the government to raise public awareness. As one civil society representative pointed out, "If the Zimbabwean government is going to move to digital identity, we shouldn't be reading it from online sources. I don't think it was even covered in the local paper".

People's understanding of the BVR system was complicated by a range of problems: political parties disagreed over private sector partners, attempts to de-duplicate voters by using BVR led to ghost voters and voter intimidation continued as ruling party officials and traditional leaders reportedly recorded the serial number on the voter-registration slip of 31% of voters.[13] All of the problems surrounding BVR created serious confusion for voters.

In one focus group many agreed that there was, thus far, a lack of public engagement and consultation regarding the transition from the old national registration system to the new biometric. Some were particularly concerned about the government's failure to communicate ID changes to marginalised groups, such as rural residents, farmers and street vendors. In an all-women focus group discussion, women noted that the government has still not explained the benefits of the new ID. Women in Zimbabwe, especially in rural areas, have little understanding of why and how the biometric ID can be used to benefit them. Although there is some awareness among people living in rural areas that there is a transition from 'traditional' metal IDs to new biometric IDs, the rationale for this transition is still not clear.

---

[11] Machivenyika, F. (2019, September 23). Biometrics to weed out ghost workers. *The Herald*. https://www.herald.co.zw/biometrics-to-weed-out-ghost-workers/

[12] Ibid

[13] ZEC later condemned this voter intimidation. See The Zimbabwe Mail. (2018, January 31). *ZEC condemns voter intimidation as polls loom.* Available at: http://www.thezimbabwemail.com/main/zec-condemns-voter-intimidation-polls-loom/

A civil society informant said the government has a tendency to cloak controversial plans under national security:

> Let's look at how little information is available around the facial recognition technology that the Zimbabwean government has acquired from the Chinese enterprise CloudWalk. So we are seeing a situation where government does things, but it doesn't report them to Parliament and it doesn't report them to taxpayers. We are seeing a very poor flow of information from government entities, especially when the information has been shrouded under a blanket of national security. If there's topics that government doesn't want to discuss, it simply labels them as national security issues, and that's very hard to get information around that.

In addition to withholding information, the government may also be taking advantage of the limited digital literacy among the ZImbabwean populace to implement a national digital ID system without much attention. This lack of technical knowledge can also be an implementation barrier, ultimately impeding the success of whatever system is eventually rolled out. A civil society interviewee explained:

> We would need to have an extensive digital literacy campaign... because look at how people are currently struggling with securing their bank cards. In the past year and a half, we have seen a skyrocketing in the number of card cloning cases, for example, and in the number of electronic or ecocash fraud, for example. So those are all symptoms of a society that does not really understand how to keep some tech-based services secure. Similarly, with digital ID, people would probably not be able to utilise it to its fullest because they don't understand it. Think about how many people have smartphones, but they only use it for SMS, for calls and maybe for WhatsApp, and the rest of the features lie neglected because people just don't know how to use those technologies.

Lack of public consultation

Several respondents in Zimbabwe pointed to the lack of public consultation as a problem and complained of a top-down approach. They expressed concerns over the lack of an official explanation on the need to change from a non-biometric system to one that gathers biometric data. A private sector informant expressed frustration with the government's failure to consult business stakeholders as well as the general public. Concerned about marginalised populations, a civil society informant said:

> I can speak of the marginalised people, probably in the rural areas and even in the Central Business District, the street vendors. They are just having those documents for the sake of having identities. There are no explanations as to why are we moving from the traditional identity documentation to the new biometric... so I think we have a problem in terms of raising awareness and also consulting. The constitution is very clear, if you are

> making certain decisions which affect the citizens, they must be consulted and have buy-in. However, it seems this is not happening, they just introduced the system. It's more of a top-down approach, which is forced into citizens.

Ultimately, Zimbabwe's lack of transparency around the digital ID system means that few people understand the purpose of biometric IDs or possess even basic knowledge of the system.

Registration barriers

Zimbabwe's biggest barrier involves registration requirements. Some civil society informants worried about the transition to digital ID given that a "number of Zimbabweans right now actually don't have identity", meaning that they are not in possession of identification documents. In fact, the country's Human Rights Commission announced in June 2019, soon after our field research phase, that they would conduct an inquiry into the unavailability of "identity documents – including birth certificates, national IDs, passports, citizenship for those formerly known as aliens and death certificates".[14]

With the move from metal to plastic biometric cards, people continue to face difficulties with the initial verification of their identity due to errors on existing documents, such as birth certificates, or lack of information relating to their origins, such as village of origin and name of local chief. One person explained their hunt for required documents:

> If your birth certificate gets lost here in Seke, they will refer you to the National Registry Office at Makombe because their information here is not online. At Makombe, the process is very long and tiresome: they first have to search your name from the computer. You will be unfortunate to be told that your information is not at Makombe but in Marondera. You will be given a phone number to contact the officers there at your own expense. If you make a call, you might be put on hold until your airtime is finished. If you request the officers at Makombe to make a call using the office landline, they will demand a bribe first.

Having errors on birth certificates corrected is also costly, and some people said they could not afford to pay for a replacement. As a result, they have gone without proper identification. People in focus groups described the way people are treated at the Registrar General's Office. Said one participant, "So many people are not comfortable visiting those offices that they have gone many years without rectifying their documentation problems because of fear of harassment". This problem indicates a need for better training and grievance-reporting mechanisms.

Queues for IDs in Zimbabwe are long. Often, more people show up to register than officials can handle in one day, forcing them to issue numbers on the spot and take people in that order:

---

[14] Nyamukondiwa, W. (2019, June 18). National documentation inquiry on cards. *The Herald.* https://www.herald.co.zw/national-documentation-inquiry-on-cards/

> If they were only taking 50 people per day and you are number 51, you will no longer be entertained and that number will not be useful the following day. The next day you should be early as well so that you can secure any position between one and 50.

After travel and long waits, people sometimes got to a registration or records desk only to encounter network problems. One civil society representative said that lack of reliable internet access extended the duration of the registration process.

Additionally, transgender people in particular have faced significant registration barriers, a problem that is unlikely to be rectified with the new digital ID system. In one case, a gender and sexual rights group described how the Registrar General's Office harassed one of their members for producing a birth certificate stating they were male while they appeared female. For this person to obtain their ID, the Zimbabwe Lawyers for Human Rights had to step in. An organisation that works with the LGBTIQ community told us that transgender people are often treated disrespectfully by authorities, who make a point of looking repeatedly between their bodies and identification documents while questioning their gender.

These experiences highlight how existing prejudices can be exacerbated ID systems. As more people register, especially those who have been excluded from previous ID systems, more discriminatory situations will arise. Without proper processes and training to acknowledge the wide diversity of lived experiences, digital ID systems will not meet the needs of people most in need of their potential benefits.

Lack of informed consent

A major concern that came up in focus group discussions was the notion that agreeing to enrol for a biometric ID automatically translates to consent for the government to share personal data with various public and private entities for surveillance. Another civil society representative suggested that "consent has to be active in each and every stage", and most focus group discussions around this issue focused on trust.

While a few people said they trust the government with their data as long as the information is being requested in a proper government office rather than someone coming door to door, most people we interviewed expressed concerns that their data may be used or shared without their consent. Activists in particular feel that their data is not safe with the Registrar General's Office. During their focus group discussion, farmworkers spoke of the desperation for aid that drives them to rely on the government despite their misgivings: "No we don't trust them. We just give them our data for survival, and we are pushed by starvation."

If the choice is between starvation and handing over data, there can be no meaningful informed consent. Problems with consent and trust can have an impact all Zimbabweans, but people in need of life-saving aid distributed with the use digital ID are most affected.

Lack of data protection and fears of surveillance

In October 2019 President Emerson Mnangagwa's cabinet approved an omnibus Cyber Crime, Security and Data Protection Bill, sending it to Parliament for debate.[15] While the country is in need of a data protection law – the 2002 Access to Information and Protection of Privacy Act being fairly irrelevant given the use of new technologies – many have criticised this bill.[16] The draft omnibus merges three bills, each of which could have been stronger if passed separately. Although the bill was approved after our field research, the draft was originally introduced three years ago. Our focus group discussions and interviews on data protection remain relevant since Zimbabweans are still operating without sufficient data protection.

Aside from the problem of potentially sharing data with other countries through commercial partners in digital ID design and implementation, focus group participants in Zimbabwe had significant concerns about data sharing within their own country. For example, farm workers expressed concerns about surveillance by uniformed forces including the police and military. Activists, on the other hand, expressed concerns about their data being shared with political parties. Sex workers, people from the LGBTIQ community and people living with HIV feared data sharing amongst government, the police, certain NGOs and churches. Churches, in particular, are seen as a threat, in regard to health information that congregants share in confidence for support. Some churches were also said to discriminate against people with HIV/AIDS.

In short, almost every group we spoke to was afraid of what those who wield power over them would do if they had access to their personal data. A civil society interviewee summed up these concerns in relation to human rights:

> [D]igitalization is a noble idea in terms of efficiency and reduction of crimes, but we are worried by the secondary use because the moment that government has all data for everyone, it might be used to... suppress dissent. [The] economic situation is becoming difficult. People will end up demonstrating, exercising their constitutional right, but the moment that you participate in that and the fact that there are cameras and all our data is in the hands of the Registrar and the state security, it becomes difficult. We will be hunted down before even we know that we being looked for.

Thinking about how institutions profit off of data, one focus group participant noted that they preferred sharing their data with the government than with the private sector. Although this person said they did not trust the government, they were convinced the state had the potential to implement safeguards that many companies may ignore.

---

[15] Mudzingwa, F. (2019, October 9). Cyber crime bill finally gets cabinet approval. *Techzim.* https://www.techzim.co.zw/2019/10/cyber-crime-bill-finally-gets-cabinet-approval/

[16] MISA Zimbabwe. (2018, February 3). Omnibus cyber bill muddles fundamental rights. https://zimbabwe.misa.org/2018/02/23/omnibus-cyber-bill-muddies-fundamental-rights/

Participants also shared concerns about dating sharing amongst government departments, healthcare providers, and various private sector parties such as financial institutions. As one civil society representative explained, if a car insurance provider has access to health information detailing medical conditions such as epilepsy, the provider might increase that person's premiums. Additionally, several interviewees were convinced the government already obtains personal information from banks. These comments echo trends in other countries, where the private and public sector use personal data to derive 'insights' that affect people's ability to access other services.

Zimbabweans have already expressed suspicion about the way the government accesses and uses their personal information. During the 2018 elections, there were instances of people receiving SMS messages that appeared to come from the ruling party, including messages encouraging people to vote for a particular candidate. The messages contained information about each recipient, including accurate details on the council and parliamentary representative running for election in their residential area. On social media, people complained that they had not given their contact information to the ruling party and were concerned about politicians having such access.

Through our interviews, it became clear that people's experiences with technological surveillance affected their opinions of digital ID. Their lack of trust in how the government treats their personal data reflects suspicion of the digital ID system. One focus group participant described the digital ID plan as part of "the militarisation of this country", and while many participants could see digital ID and facial recognition making streets safer, they also expressed fears about surveillance. A male sex worker stated:

> Security operators will now be aware of my daily movement patterns, and they may have targets in a community. My information might be used for other purposes than it was captured for by other institutions, such as the police.

In fact, sex workers, activists and women living in an informal settlement were particularly dismayed. They described feeling "afraid" and like their "freedoms and rights are being curtailed". Overall, most focus groups saw these technological developments as a threat to human rights even if they praised the potential benefits of increased safety and decreased fraud.

Civil society

Civil society in Zimbabwe works in a hostile environment, which makes it difficult to push back around sensitive issues such as the country's digital ID efforts. This is further complicated by the fact that digital ID is seen as a 'national security' issue. A participant in a focus group discussion with civil society stated:

> Any civil society organisation [that chooses to address digital ID]... will be drifting into national security terrain, and that will definitely raise attention from the government, from

> national security agents, and even get people from those civil organisations called in for interviews, prodding and intimidation and all that.

Civil society informants told us, however, that there was a need to "broaden their work to include" issues around digital ID and act as "watchdogs to ensure the government does not abuse digitalisation". They also felt that they had a responsibility to educate the public about the benefits and risks of digital ID and to lobby for legislation that protects people's data and their right to seek redress for misuse. MISA Zimbabwe is cited as an example of an organisation that has been taking action against the government's use of emerging technologies to expand surveillance.[17]

Conclusions and recommendations

Zimbabwe presents a particularly indicative case of future digital ID trends. In particular, the initial involvement of Chinese companies demonstrates the value of Zimbabweans' data to foreign governments. Although many advocates and experts have criticised racial discrimination in emerging technologies like artificial intelligence, here is a case where increased diversity in training data can cause increased harm by contributing to the curtailling of Zimbabweans' data and privacy rights.

The risks of digital ID and related technologies are most severe for people in Zimbabwe whose rights and livelihoods are already systematically denied or questioned, such as transgender people and sex workers. Though the intent of many digital ID systems is to include people who struggle to access 'traditional' identification documents, these systems appear to have strong potential to further exclude.

Additionally, Zimbabwe's political environment of increased militarisation and shrinking space for civil society means that trust in government is low, and the impression that the digital ID system fits into the narrative of national security means that civil society involvement is made more difficult. While it is difficult for civil society to take action in this environment, it is also vital because these organisations and associated human rights defenders are likely to be targeted by digital ID and other surveillance technologies. If these systems are used to crack down on rights such as freedom of assembly and freedom of expression, the ability of civil society to create change on any issue will be radically reduced.

If digital ID must go forward, Zimbabweans can benefit from a system that puts the needs of people first and recognises the diverse contexts of marginalised populations. In place of a weak omnibus bill, robust data protection that affirms people's rights and includes enforcement mechanisms can significantly boost trust in both the system and the government. Finally, public

[17] Maunganidze, G. (2018, December 4). Letter to Speaker of National Assembly: Increase in collection of personal information in the absence of adequate data privacy legislation. MISA Zimbabwe. https://zimbabwe.misa.org/2018/12/04/letter-to-speaker-of-national-assembly-increase-in-collection-of-personal-information-in-the-absence-of-adequate-data-privacy-legislation/

consultation and awareness campaigns can also build trust while helping people get the most out of digital ID.