Identified but Unheard

Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalized Communities

Priyal Bhatt, Sarah Moulton, and Elizabeth Sutterlin
National Democratic Institute

June 2021

NDI DEM TECH NDI

Table of Contents

Executive Summary

Digital ID systems promise to make life easier. With a digital ID, in theory, opening a bank account or accessing an agricultural subsidy is more efficient. But questions of who controls information collection, where data is stored, and how data is used present tremendous challenges for democracy. Digitally streamlined and interconnected systems, when designed inclusively and implemented with appropriate legal frameworks for data protection, can broaden opportunities for civic and political participation. Yet these centralized identification systems can just as easily be used as a weapon to coerce specific communities, perpetuate existing inequalities, and reinforce discrimination against marginalized communities who have been historically excluded from exercising their civic and political rights.

The goal of this paper is to understand how digital ID systems can impact individuals' abilities to exercise their civic and political rights, particularly for members of marginalized communities, and to provide recommendations for building inclusive, secure, and transparent ID systems. Despite a large body of research on digital ID's impacts on social and economic inclusion, a gap around the impacts on political participation remains. As governments digitize identification systems and electoral procedures and seek to connect them, it is crucial that any digital ID system upholds democratic principles of inclusion, privacy and security, and transparency.

To answer these questions, NDI conducted qualitative research throughout fall 2020 and spring 2021 and developed three country case studies, attached as appendices. The findings from this research indicate that:

- Sufficient community consultation with marginalized groups during the design and rollout process of a digital ID system is needed to ensure that potential barriers to uptake for marginalized populations have been addressed. Building the capacity of civil society to monitor civic outreach and procurement of digital ID systems is an important step in creating mechanisms for transparency and accountability.

- Education on digital ID is a necessary part of deployment. Information on the purpose and registration process of digital ID systems should be made accessible and understandable for *all* members of the public, especially marginalized populations.

- Strong and enforceable legal frameworks for data privacy and security should be established before implementing a digital ID system to ensure inclusion and protection of marginalized populations who face amplified data risks and fears of surveillance.

- As digitized biometric voter registration (BVR) technology becomes more widely implemented, additional research on its impacts on voter marginalization and disenfranchisement will be necessary.

Acknowledgments

NDI would like to acknowledge the contributions of several individuals and organizations that have been instrumental in the development of this paper, and while we cannot name them all, we did want to thank a few who made particular contributions.

The approach and methodology of this paper has benefited from a vast body of existing research on digital identity, including studies conducted by The Engine Room, the United States Agency for International Development (USAID) and the Center for Global Development.

We owe a debt of gratitude to Amine Ben Naceur, Amanda Manyame, Jimmy Kainja, Daniel Ukpai, Uge Timipanipre, and Summer Boucher-Robinson. This paper would not have been possible without their research contributions. We are also grateful to the International Foundation for Electoral Systems (IFES) for contributing their expertise on biometric voter registration to this research.

We would also like to thank NDI staff on the following teams: Democracy and Technology; Gender, Women and Democracy; Citizen Participation and Inclusion; Southern and Eastern Africa; and Central and Western Africa. We appreciate your guidance and contributions throughout this project.

We deeply appreciate the many civil society leaders, digital rights experts, and government officials in Nigeria, Zimbabwe, and Malawi who shared their knowledge, time, and experiences with us. Most importantly, we are greatly indebted to the individuals who shared their lived experiences with us in interviews, surveys, and focus groups. Thank you for sharing your stories.

Background and Introduction

How do governments around the world develop and maintain registries of their populations? In some countries, paper-only national birth registries still exist. But as of 2018, 161 countries had introduced some digital components to their identification systems. Digital identity systems have the potential to revolutionize political and economic inclusion around the world. Still, over one billion people worldwide lack access to any form of official legal identity.[1]

Legal identification empowers an individual to exercise their economic, social, and civil rights in everyday life, enabling them to travel, utilize social services, receive medical care, open bank accounts, and access the internet. Those without proof of legal identification can be barred from these activities, as well as from the fundamental processes that form the basis of a democracy, such as voting, running for office, or participating in the political life of their community. The relationships between legal identity, health and education outcomes, and participation in economic and political life are so established that the United Nations developed a Sustainable Development Goal (SDG) aimed at providing legal identity to all people by 2030.[2] Expanding responsible access to identification, digital or otherwise, is crucial to address global inequalities.

In this paper, digital ID systems are defined as identification systems that use digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer, for credential management, and for identity verification and authentication.[3] Common examples include national identity cards issued by countries in the European Union, or India's Aadhar system. While the benefits of an identification system can be brought to bear whether that system is digital or paper-based, digital ID systems are unique in their connections to streamlined and automated components not encompassed by analog ID systems. Where this paper discusses biometric voting technologies, it refers only to digitized biometric records (such as fingerprints or iris scans) and their connections to digital identity, not to traditional paper records of fingerprints or other records of biometric identifiers.

Digital ID systems, purported to be more efficient than their paper predecessors, are attractive to governments looking to bring in new revenue from taxes, decrease duplicative welfare and social spending by expanding the population of citizens with proper legal identification, provide for national security and protection of citizens, signal a business-friendly environment to investors, or demonstrate their own innovation through novel digital programs to bolster confidence in a leader or party.[4] [5] [6] International aid organizations have directed resources to help states implement digital ID systems with the goals of improving government service delivery and development outcomes, particularly for marginalized populations. In this paper, marginalization refers to a situation in which a group, a demographic, or selection of people are treated as inferior, insignificant, or lesser because of their association or identification with that group. Marginalization results from persistent inequality and adversity resulting from discrimination, social stigma, and stereotypes. Individuals can face multiple forms of marginalization. Women, for example, face additional gender-based barriers to obtaining legal identification, which are compounded for women who are marginalized for other aspects of their identity, such as disability status.[7]

The wider access to legal identity that digitization of these systems could facilitate will likely increase the number of people worldwide who are able to exercise their civic and political rights. A 2007 study from NDI and the Latin American Faculty of Social Sciences found that lack of proper identification was the main reason that Indigenous voters in Guatemala voted at a significantly lower rate than other ethnic groups.[8] A digitized system promises to bring increased ease of access to identification, services, and democratic processes for marginalized communities who may have had difficulty accessing them in the past.

However, introduction of a system without careful, inclusive planning can also amplify and reinforce existing inequalities and introduce new challenges for data privacy and security. While some risks to personal data existed in older, paper ID systems, the ability to collect and connect disparate data points in seconds introduces new potential for harm such as surveillance, discrimination, and disenfranchisement. As digital identity systems and biometric voter registration (BVR) become the primary ways for citizens to register and vote in elections, a non-inclusive and non-trusted digital ID system could bar marginalized communities from exercising their rights to have a voice in their governments.

Digital ID Adoption in the Global Community

Digital ID systems can be incredibly complex projects implemented by a number of stakeholders from across the public, private, and non-profit sectors. Each stakeholder has unique goals in driving the adoption of digital ID.

International aid organizations like the World Bank and the UN Development Programme have led the charge to digitize identification systems in a number of countries.[9] [10] Such organizations assist national governments in the implementation of digital identity systems and work to ensure systems adhere to global best practices and standards for data protection and privacy, though these partnerships are often non-transparent to the average citizen.[11]

National governments around the world have embraced the transition to digital identity systems under the auspices of everything from economic development to national security, from anti-corruption to nation-building.[12] Without a reliable database of who lives in a country, many governments claim that it is difficult to raise revenue through taxation, to ensure the distribution of social services and benefits, to eliminate corruption, or to prevent voting fraud or manipulation during elections.

Private sector companies have been large drivers of digital identity adoption for several reasons. Locally, banks and financial services benefit from streamlined, centralized digital identity systems, which can reduce financial fraud and make it easier for banks to comply with Know Your Customer (KYC) laws.[13] The Global System for Mobile Communications Association (GSMA,) which represents a global network of mobile operators, provides significant funding for the development of mobile-enabled digital identity systems.[14] International multinational corporations work with national

governments and international aid organizations as system vendors and as contractors to implement digital ID systems.

Civil society organizations (CSOs), on the other hand, have been divided on the relative benefits and threats presented by digital ID. While digital identity can create opportunities for non-governmental organizations to provide higher quality services to the communities they serve, many groups have expressed concerns about what governments will do with the data collected in these databases, particularly the data belonging to members of opposition groups or marginalized communities. CSOs may be able to play a crucial role as implementers and monitors by improving access to identification among communities they serve, by monitoring the digital ID implementation process, and by exerting pressure on other stakeholders to improve data privacy and security measures before those who enroll are exposed to harm.[15]

Research Scope and Methodology

Civic participation and inclusion are cornerstones of a healthy democracy, and it is crucial that the digitization of any public service or system builds on these cornerstones, rather than wearing them away. While much of the focus of current digital ID research centers on the health and economic impacts of these new forms of identification, this white paper takes a closer look at the ways in which implementation of biometric-based identity systems may impact individuals' civic and political rights and participation. This paper takes into special consideration the impact of these systems on the rights of marginalized individuals, and how the design or rollout of biometric-based systems can potentially reinforce or create new forms of exclusion.

Background research for this paper draws from a number of existing digital ID resources, including the World Bank's Identification for Development (ID4D) initiative, The Engine Room's report and in-depth case studies on lived experiences with digital ID, the work of signatories to Access Now's #WhyID Initiative as well as the Center for Global Development's working papers on biometrics and the ID revolution.[16] [17] [18]

To augment its global literature review, NDI conducted qualitative research (a combination of interviews and focus groups) in Malawi, Nigeria, and Zimbabwe to understand a cross-section of perspectives from those involved with the rollout of digital ID processes. NDI also conducted an online survey about individual experiences with digital ID systems, which received responses from individuals in Albania, Georgia, Ghana, Indonesia, Malawi, Morocco, Nigeria, Rwanda, Serbia, Uganda, and Zimbabwe. Altogether, NDI gathered feedback from 55 individuals, including government officials and digital rights leaders, as well as representatives of marginalized communities. The selection of countries for case studies was based upon NDI's field office presence in each location, as well as long-standing relationships with its partners, which facilitated the discussion of sensitive subject matter, such as perceived discrimination, aspects of data privacy, and concerns about retaliation based on political preferences.[19] Each of these three countries is at a unique stage of national digital ID implementation, and has taken a different approach to digitizing its national ID systems. Variation across country contexts provides a richer understanding of what factors may contribute to a more inclusive digital ID system globally.

The first section of this paper provides context about digital ID adoption in the global community, and provides an overview of key considerations for inclusive design and addressing the data risks associated with digital ID systems. The second section takes a closer look at how issues around digital ID are amplified when systems are linked to the electoral process, either through BVR or other databases, introducing the potential for digital disenfranchisement. Case studies, attached in appendices, look more closely at each of these issues in a specific country context.

Designing Digital ID for Democracy

The design of a digital ID system plays an important role in creating positive opportunities but can often augment the power and influence of political elites and exacerbate existing inequalities.

Designing an Inclusive Digital ID System

Enrollment in a digital system can be mandatory or voluntary. Compulsory enrollment not only limits user agency and choice, but can also have more damaging exclusionary effects.[20] In these cases, the inability to enroll in the digital ID system, whether by choice or due to a lack of documentation, limits the availability of essential services or subsidies.

While many countries implement nominally voluntary systems, these voluntary digital systems are not necessarily truly optional. In many places, digitized identification is now required for everyday banking transactions or SIM card registrations. In Nigeria, digital rights experts noted the public outcry and fears surrounding the Revised National Digital Identity Policy for SIM Card Registration, which requires the linking of national identity numbers to SIM cards.[21] In these contexts, the costs of not enrolling in the digital ID system are so high that those with reservations about privacy and security are compelled to enroll anyway. These high costs of non-enrollment can further inequalities and contribute to a vicious cycle of poverty for vulnerable communities. In one stark example, India's application to register for the COVID-19 vaccine requires users to be registered in Aadhar, the country's digital ID system, therefore excluding millions of individuals from getting the vaccine who are not enrolled in the Aadhar system.[22] In a survey question on the motivation for enrolling in their country's digital ID system, respondents overwhelmingly referenced needing a new digitized ID card to access a specific service as the driving reason for enrollment.[23]

Include Public Consultations in the Design Process

As with any national project or campaign, digital ID programs benefit from participation and collaboration from diverse communities in the design process. This type of inclusive consultation process embodies the principle of designing "with, not for," the community and ensures the systems work for all stakeholders, especially marginalized populations.[24] Community consultations can help system administrators proactively identify blocks or issue areas that will discourage or prevent

individuals from participating. Inclusive community consultations also open doors for dialogue and lead to more trust and buy-in to a system's purpose, benefits, and potential risks. However, inclusive community consultations are not always the norm, and marginalized communities may not be consulted during the design or implementation of a digital ID system.

Many countries, such as Ghana and Kenya, have often cited national security rationales as a reason for the lack of transparency in the design of their digital ID systems.[25] However, without thorough consultations with diverse perspectives, important community needs are not considered. As a transgender survey respondent from Ghana summed up, "there are a vast number of minority-led organizations, human rights and gender advocates in the country [Ghana] who would have provided accurate information to influence the digital ID programming."[26] In cases where collection of gender information or identity documents become roadblocks to equitable enrollment of the LGBTQI+ community, organizations that serve affected individuals can offer guidance on avoiding these pitfalls. Similarly, organizations working with persons with disabilities (PWDs) can offer guidance on accessibility of enrollment centers and civic education materials. Women can help identify both physical and social barriers to access, such as enrollment center hours and location, or patriarchal norms that perpetuate a gender divide in ID access. If included in the process, marginalized communities have the opportunity to preemptively identify and mitigate these barriers to participation.

Community consultations can play an important role in demystifying complex and technical systems and increasing transparency and trust. Survey respondents noted they did not have access to enough information on the purpose of digital ID, its benefits, and potential risks.[27] Insufficient information can lead to a lack of trust as to why certain data is being collected and what happens to that data. Interviews with digital rights experts in Nigeria noted a prevalent belief among Nigerian citizens that the government's current push for digital ID aims to monitor citizens in the face of growing dissatisfaction with government, such as the recent #endSARS protests.[28] Without community participation or strong civic education efforts to bring transparency to the structure and controls on a digital ID system, perspectives based in fear and misinformation can flourish.

Deploy with Accessibility and Inclusion Considerations

In addition to a consultative design process, an effective digital ID system must consider accessibility and inclusion needs during the implementation phase. Persons with disabilities can face significant accessibility barriers when registering for a digital ID. Factors such as the locations of registration centers, long wait times, and the ability of staff to accommodate special needs can influence the ease of the enrollment process. For women and for people in low-income or rural communities, taking time off of work, finding childcare, and securing transportation to and from the registration site can be cost-prohibitive, creating additional barriers to enrollment.

Many of these barriers in digital ID registration can be identified and preemptively addressed through community consultations in the design process, often through innovative accessibility solutions. In one such case, the Philippines opened national ID registration centers in shopping malls, improving communities' access to enrollment sites by putting them in locations that are familiar and easily

accessible by public transportation.[29] Other countries have linked mobile registration drives to other key events, such as an upcoming election, in order to encourage registration. In Zimbabwe, the Registrar-General's department held a mobile registration drive to promote national identity card enrollment ahead of the 2018 voter registration exercise, for which prospective voters would need to show proof of identification.[30] These approaches can play an important role in lowering barriers to participation.

Addressing the Data Risks of a Digital ID System

While digitizing national identity databases can bring enormous benefits, a national database of personally identifiable information (PII) also poses significant risks if not accompanied by a corresponding legal framework that covers the collection, sharing, retention, and management of sensitive personal data. There are risks inherent to any database architecture, and while centralized databases can be more secure than decentralized ones in many scenarios, a central storage location for the personal data of an entire population may become a higher-profile target for cyberattacks and hacking if not properly secured.[31] The likelihood of these threats occurring increases when the officials responsible for administering and managing these data systems are not data-literate or cognizant of the real-world implications of data breaches, such as identity theft and financial harm to the users whose data is compromised.

In an era of rapidly spreading digital authoritarianism, a sufficient data protection regime and comprehensive legal framework for digital ID are necessary to guard against government and corporate surveillance, extractive data collection practices, and offline harms for opposition parties, human rights defenders, activists, and many others. The inherent risks of national databases of sensitive information are amplified for vulnerable populations. These risks often have a chilling effect on the ability to register for a digital ID card or to access the benefits of digital ID: groups who are already the most concerned about the personal or reputational risks stemming from surveillance or data breaches are less eager to willingly submit to those risks. A strong and transparent data protection regime that protects sensitive information of marginalized groups is crucial for the implementation of a digital ID system that is inclusive and democratic.

Administrative Training for Digital ID Data Management

Government officials responsible for national ID database maintenance must be adequately trained on how to safely and securely collect, store, and manage personal data and biometric information. Inadequate training can lead to instances of both intentional and unintentional data sharing and data breaches.

Comprehensive standards for database managers and administrators are particularly important for digital ID systems where biometric data is stored, whether that data contains iris scans, fingerprints, facial recognition, or other forms of unique personal information. While biometric identification is hailed over traditional passwords as a way to verify identity and provide account security, the uniqueness of these identifiers necessitates thorough protection. Unlike an account password,

people can not change their facial structure or fingerprints if hackers or other malicious third parties gain access to a database and compromise that information. To prevent such a breach from occurring, digital ID databases that contain biometric information must be appropriately protected and secured. That protection includes transparent and enforceable standards for those who administer and manage such databases.

Strong Legal Frameworks for Data Protection and Digital Rights

Strong and transparent legislation regarding data sharing and protection is necessary for citizens to know who has access to their personal information, and thus to give informed consent to their inclusion in such a database. Gaps in legal frameworks around digital data or insufficient data privacy and protection legislation, such as a lack of mechanisms for independent and robust enforcement of laws, for data breach prevention and notification, or for secure data transfer to third parties and countries, can leave doors open for intentional misuse of data by authoritarians seeking to limit competition and stay in power.[32] The likelihood of these risks to digital rights only increase as the pandemic accelerates the adoption of new surveillance tools and the decline of internet freedom around the world.[33]

While government surveillance and digital repression are major concerns, this is not the only data risk facing people who enroll in national digital ID systems. Almost all public-sector digitization initiatives involve a high degree of public-private partnerships, particularly in emerging economies. In some cases, the contracts for constructing databases of sensitive personal data are awarded to large multinational corporations, who may be less accountable than governments to the people whose data are collected and stored in these systems.[34] Multinational technology corporations like Microsoft have worked to implement digital identification in humanitarian crises as early as 1999, raising questions about system and data ownership.[35] Whether technological or financial, dependence on third parties can call into question the legitimacy of a digital ID system as a public good. Concerns about profit-driven ulterior motives can depress interest in registration. In Nigeria, for example, civil society members expressed concerns about opening up Nigeria's National Identity Management Commission (NIMC) to foreign sponsors (including MasterCard), although corporate sponsorship would provide financing to make an operational digital ID system a reality.[36]

In Zimbabwe, a partnership between the government and a Chinese facial recognition technology company sparked media attention, due to the perceived potential for both private and public sector data exploitation.[37] Given the strength and extent of the Chinese Communist Party's (CCP) surveillance and censorship regimes at home, the government's partnership with an AI company with ties to the CCP raised concerns of surveillance as well as the possibility of a foreign government obtaining access to a national database of biometric identifiers. Without clear legislation on where data can be transported, shared, and stored, companies accumulate vast amounts of personal information at little to no cost and earn financial benefits from proprietary algorithms, without providing fair compensation to the people whose data creates algorithmic value, in a process known as data colonialism.[38]

Addressing Scope Creep Concerns around Digital Identity

The pace of digital change is rapid and still accelerating. As new applications for data and new methods to utilize it come into play, there may be opportunities for governments with comprehensive national ID databases to apply this information to new agencies and public services, and to use data to face new challenges. These opportunities also carry risks to data privacy, safety, and inclusion, particularly if a system designed for a particular use case expands in scope without a legal framework that is prepared to address new applications of a national digital ID database.

A lack of transparency about who has access to the PII captured in digital ID databases, at best, infringes on people's right to make informed decisions about their own information and privacy. At worst, it has severe consequences that contribute to exclusion and discrimination from institutions and public resources. Information that is initially submitted to specific agencies can produce concrete harms when shared across government without consent, such as with security or immigration agencies. Invasive data sharing practices with police or security forces may infringe on people's right not to be searched without a warrant. In closed and closing spaces, where government ministries act as an extension of a ruling party, the sharing of sensitive health, financial, voting, and other personal information across agencies could pose severe security risks to activists, members of opposition parties, and human rights defenders.

These risks of discrimination and exclusion are amplified for members of marginalized communities, who in many cases are cognizant that they lack knowledge about how their data is managed and protected. In countries with histories of biased policing, the sharing of sensitive personal data with security forces without warrants may exacerbate discrimination and inequalities. LGBTQI+ people also face risks when their data is unknowingly shared. LGBTQI+ survey respondents in Ghana and Uganda expressed hesitation about sharing sex and gender information with government bodies when registering themselves in their countries' digital ID systems.[39] If such sensitive information is mandatory for registration, and people fear that disclosure could lead to discrimination or prosecution, they may choose to avoid registering altogether. As digital ID systems become the main vehicle for government service delivery, and as some countries begin to mandate registration, this would lead to unjust exclusion of marginalized groups from access to government services, voter registration, and the full suite of benefits that digital ID proponents claim such systems will provide.

Scope creep in the usage of PII can occur anywhere, but a strong legal framework that protects human rights can mitigate the dangers of non-transparent data sharing agreements or the outright misuse of PII. In Switzerland, after civil society groups challenged a law that would establish a government digital ID system primarily managed by private companies, a popular referendum resoundingly rejected the proposed system. Those on the referendum committee found that mistrust of companies drove the results, and that voters were open to a digital ID system so long as it was fully managed (not just licensed) by government and under democratic, rather than privatized, control.[40] Similarly, a legal challenge in the United Kingdom was able to halt the extension of an agreement between the National Health Service (NHS) and U.S. tech company Palantir, after a proposed deal would have continued to share an enormous database of sensitive health information with third parties after the COVID-19 pandemic subsides.[41]

In countries with high rates of digital literacy, long histories of democratic participation, and established legal frameworks that defend the rights of the individual, government representatives are accountable to an informed public before making long-term agreements on data collection, management, and sharing. However, in contexts where any of these factors are lacking, civil society and the broader public may have less awareness of and less ability to weigh in on the agreements between governments and companies about how PII is shared and used.

Connecting Digital ID to the Voting Process

National ID systems vary significantly in the type and scope of government services available upon enrollment. While access to health, transportation, and social security benefits tend to be common, only 11% of the global population has a national ID (either digital or analog) that enables voting.[42] However, pressure to address concerns around election integrity (often by international actors) may prompt a government to prioritize the adoption of biometric-based voting technology prior to, and independent of, putting a centralized digital ID system in place. Today, over 38% of countries now capture some form of biometric data during the registration process (i.e. fingerprint scans and/or photos). Among countries in Africa, over half (52.7%) collect the biometric data of voters.[43] Although donors continue to provide funds for biometric voting technologies, high costs per voter and sustainability challenges associated with single-purpose systems may incentivize both donors and recipient governments to find ways to integrate voter data into existing or proposed digital ID systems instead.

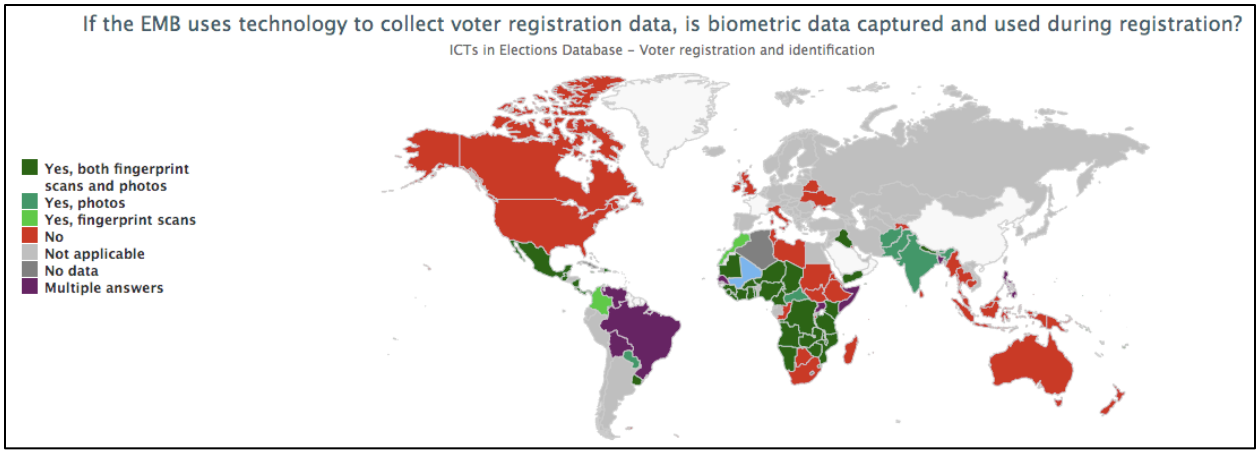

Figure 1: Countries in which an Election Management Body (EMB) uses biometric data to collect voter registration data *(International IDEA)*

Digital biometrics-based approaches used for the voting process often come with the same implementation challenges and unintended consequences as national digital ID initiatives: lack of community input, opaque data collection and management standards, inadequate information sharing, and unequal access. These factors can exacerbate risks for potential voters already marginalized due to social, economic, or political factors, or for those living under authoritarian political regimes. For such populations, if sufficient measures are not taken to build public trust in a

system, or to ensure that sensitive voter data remains confidential, the risks of further voter disenfranchisement increase, and the legitimacy of entire electoral processes may be called into question.

Biometric Voter Technology and Voter (Dis-) Enfranchisement

Beyond its potential as a tool for reducing election fraud through elimination of duplicate or deceased voters, biometric voting technology is often touted as a mechanism for enfranchising all eligible citizens by modernizing the register and instituting new processes to reach those who may have been excluded from previous registration exercises due to factors such as gender identity, disability, geographic location, and ethnic or religious divides.[44] In conflict-affected states or transitioning democracies, the perceived legitimacy and neutrality of a biometric-based voter roll can increase confidence in the electoral process, potentially reducing the risk of election-based violence.[45] In countries in which a national digital ID scheme is not yet in place, registering to vote may provide an individual with their first opportunity to receive official identity documents, leading to the enfranchisement of communities traditionally left out of the voting process. In Bolivia for example, the digitization of the voter roll in 2009 expanded the number of registered voters from 3 million to 5 million, including a significant number from undocumented and Indigenous communities.[46]

Where digital ID systems are already in place, the possession of a biometric-enabled ID may also facilitate an individual's participation in the voter registration process, particularly for those previously left out of previous voter registration efforts due to lack of formal identification. However, in countries in which a digital ID system is still voluntary, or in which significant segments of the population have not yet enrolled, some are concerned that governments will nevertheless require it as a condition for registering to vote. In early 2021, the Independent National Electoral Commission (INEC) in Nigeria was forced to make a public statement claiming that the new biometric-based National ID Number (NIN) would not be a prerequisite for voter registration, after media reports came out stating otherwise.[47]

As with enrollment for national digital ID systems, the use of biometrics to register and process voters can further reinforce existing inequalities due to unequal access and inadequate accommodations made for those that need them, leading to disenfranchisement of potential voters. Depending on the system in place, the biometric data collected by an election management body (EMB) may be used for one or more purposes throughout the election cycle, including voter registration, creation of voter ID cards, deduplication of the register, and voter verification.[48] Ensuring equal access to these processes for all voters remains a challenge as deployments are often beset by poorly functioning technology, high costs of distribution into rural areas where internet connectivity or electricity may be unavailable, inconveniently located centralized registration centers, and lack of accommodations made for voters with disabilities.

Increased awareness of differential access to and ease of use of biometric systems can contribute to

the development of standards and practices that incorporate inclusion from the outset, and encourage enfranchisement of all potential voters. The World Bank has outlined a series of recommendations designed to mitigate challenges experienced by PWDs, such as: engaging PWDs directly in the testing of systems, establishing clear exception-handling and grievance procedures when the technology does not work, and ensuring systems follow accessibility guidelines recommended by the International Organization for Standardization (ISO).[49] In addition, recognizing, accounting for, and openly addressing existing cultural norms, such as a person's discomfort at removing facial or head coverings for photographs, or a reluctance to provide fingerprints due to negative associations with law enforcement, can also help address the reluctance of some communities to register.[50]

Data Protection and Trust in the Electoral Process

The data risks associated with national digital ID databases outlined in the previous section are equally applicable to systems used in conjunction with those used to conduct electoral processes. However, perceptions of mismanagement of sensitive voter data on the part of the government, or a lack of transparency regarding the procurement of equipment (as well as ownership of the data that equipment collects), can lead not only to distrust in election officials, but undermine a country's entire political process.

For vulnerable populations already wary about how sensitive personal data will be captured, used, and stored, the manner in which governments take these concerns into account can greatly impact overall voter participation. For example, explicit mention of a voter's ethnicity, gender, or religion on the ID card they use for voter registration or voting may make them vulnerable to harassment or intimidation at the registration or polling site, leading to the suppression of voting among these groups.[51] Taking into account the concept of designing "with, not for" the user described earlier, engaging with representatives of these groups early on in the design process can identify actual and perceived risks around the sharing and presentation of personal information, and identify solutions to mitigate any concerns raised long before it comes time to register or vote.

In authoritarian contexts, governments may take advantage of existing public distrust in biometric technology to limit or discourage participation in the voting process. In advance of the 2018 elections, the ruling party in Zimbabwe was accused of "instill[ing] fear in the hearts of the vulnerable rural electorate by creating an aura of mystery around [the new BVR system] so as to scare potential voters," and rumors that the system would know how a voter cast their ballot were also common.[52] Following the election, observers heard reports of "numerous incidents of ruling party or government officials demanding to see citizens' voter registration slips and saying that the new voter registration system would allow them to know how the person voted."[53] Beyond misinformation and rumors, incumbent governments may take deliberate steps to restrict voter participation, particularly among groups from whom it does not anticipate strong support. This could include limiting the number of registration sites in opposition strongholds or putting in place registration criteria that favor certain population segments over others. Excessive paperwork demands for acquiring the ID necessary for registering to vote, as well as high costs for transportation and document filing, can further disenfranchise a country's poorest populations.[54]

The provenance of the biometric systems themselves can also affect the public's perceptions of their legitimacy, especially in environments in which the independence and objectivity of the voting process is already a concern.[55] Foreign technology companies are commonly contracted to provide systems not only for collecting biometric information, but for managing and cleaning databases as well. This can lead to concerns about who "owns" the electoral process, and perhaps more importantly, who has access to the sensitive information collected using these technologies. In Zimbabwe, the government awarded a contract to the Chinese-owned Laxton Group for biometric voter registration kits used in the 2018 elections, drawing criticism from the opposition party, which questioned the company's independence due to the strong relationship between the ruling party and the CCP.[56] [57]

The type and breadth of the data collected as part of the biometric voter registration process - whether independent or connected to a nationally administered digital ID system - raises additional concerns about how data breaches may disproportionately impact certain segments of the population. As global cyberattacks that target elections and democratic processes increase, voters' perceptions that personal data is unsafe and at risk of misuse can permanently erode trust in biometric systems (national digital ID, voter registration, or others.) Should these systems continue to prevail, ensuring appropriate legal frameworks are in place to safeguard an individual's data will be paramount.[58]

Recommendations and Conclusion

Digital ID systems can play an important role in facilitating easier access to public services and civic participation. However, there are numerous aspects related to system design, implementation, and governance that can negatively impact the ability of individuals to exercise their civic and political rights, particularly for those who are part of marginalized populations. The following recommendations can help digital ID systems be inclusive and democracy-affirming.

Digital ID systems must be designed and deployed inclusively. From conceptualization to implementation, consideration must be given to the impact on PWDs, LGBTQI+ individuals, women, and other vulnerable populations. A first step is involving these groups or their representatives in the design and implementation process. Governments should involve civil society representatives in decision-making on whether to pursue a digital ID system. Throughout the design stage, governments should provide public consultation forums that allow civil society organizations and members of the public to offer feedback and shape the systems that will hold their data. Civil society can also play an important role in monitoring the deployment of digital ID systems. Building the capacity of civil society to monitor processes like civic outreach or procurement can create mechanisms of accountability and transparency.

Civic education on digital ID is a necessary part of deployment. Information on the reason for, impact of, and deployment of digital ID systems should be accessible and understandable to all members of the public. Trainings on a system and its implications should be provided to staff responsible for

digital ID registration to build the capacity to understand and explain these complex systems in simple ways. Civil society organizations, when included in design and deployment phases, can also be allies in educating the public. Materials on both the purpose of digital ID and how to register should be made available in forms that are accessible to all members of the public, including those living in remote areas and PWDs.

Digital ID systems should be implemented only after strong data privacy and protection practices are established. Strong, enforceable data privacy and protection frameworks are a prerequisite for inclusive digital ID systems. Information on what data is being collected, why that data is being collected, and what happens to it should be publicly available and easily understandable to all members of the public. Governments have a responsibility to be transparent with the data collection and storage processes. Digital ID systems also often start with a narrow focus and grow to provide additional services over time. Data protection and privacy legislation should continue to adapt to address concerns over growing scope. The potential dangers of surveillance disproportionately impact and can further exclude marginalized individuals from participating and reaping the benefits of a digital ID system. While not all digital ID systems are mandatory, any digital ID system that requires people to choose between their right to data privacy and their right to be included in political and economic life is not truly voluntary, and will exclude those who feel the need to protect themselves from surveillance.

Further research on the impacts of digital ID and BVR. While this paper provides an initial overview on the linkage of digital ID systems with voting processes, additional analysis on the factors that lead to the marginalization of voters will be necessary to understand the impacts of BVR as it becomes more broadly implemented.

Conclusion

The global discourse on digital identity will continue to shape not only the design and deployment of digital ID systems, but the very windows of democratic opportunity worldwide. Countries where the public and civil society have a voice in shaping their digital identity systems will enable a virtuous cycle and create environments for open political participation. However, in many countries, a lack of transparency, insufficient access to information, and exclusion from involvement in decision-making around who can access identification will beget a less participatory and transparent digital ID system that further undermines inclusive political participation and democratic principles. Trust is the foundation on which voting and other political participation occurs, and these recommendations are vital steps towards increasing trust in digital ID. Without these considerations, the linkage of digital ID systems with voter registration has the potential to severely chill the political participation of marginalized individuals today, and exclude the marginalized from exercising their civic and political rights well into the future.

Appendices

Case Study: Inclusive and Exclusive System Design in Malawi

Malawi's overhaul of its National Registration and Identification System (NRIS) introduced a smart identity card with a scannable chip that contained biometric information and applications linked to the national identity system, e-health system, e-driver's license registry, and public key infrastructure.[59] The NRIS ID card was the primary form of identification accepted by election officials in Malawi's 2019 election cycle. Malawi's National Registry Bureau (NRB) succeeded in its goal to register nine million adults by November 2017.[60] However, concerns over the integrity of electoral data and questions about the long-term sustainability and financial accessibility of the ID cards have undercut efforts to design and deploy an inclusive digital ID system.

Public Awareness and Trust

Although Malawi's NRIS reached its registration number goals in 2017, a lack of clear public understanding of the uses of the digital ID system hindered adoption and usage of the ID. An NDI interview with the UNDP, which assisted the government of Malawi to design and deploy the NRIS, noted that the public generally lacked an understanding of the scope of the new identification system.[61] Focus group discussions revealed that this lack of understanding was due in part to incomplete coordination among different government agencies and private institutions on the implementation of the new ID cards. Not all service providers, such as hospitals, accepted the new cards as valid identification.[62] Other interviews noted that laws were not amended to update voter registration requirements from drivers' licenses and passports to the new ID cards.[63] The lack of clarity on uses for the new ID and the difficulty of locating accurate information about the system led to public confusion that lowered usage rates.[64] Survey respondents from Malawi indicated the public would have benefited from a more confidential registration setting and more details on data protection.[65]

Public perceptions of the NRIS as easy to abuse in electoral contexts, identified across expert interviews and survey responses, may also have discouraged some of the public from utilizing the digital ID.[66] In a country with a history of vote-buying and other unfair election practices, the Malawian public is cognizant of opportunities that a digital voting system may provide to politicians and parties seeking to influence electoral outcomes.[67] [68] This hypothesis was borne out by evidence from NDI surveys. Respondents in Malawi who expressed discomfort with linkage of the NRIS to voting processes did not take issue with using BVR to verify their identity; instead, they were concerned about linkage between their identity and their voting history.[69] Perceptions that politicians were misusing the NRIS for political purposes undermined the credibility of the entire system.[70]

To ensure that an ID system can achieve its goals, merely introducing the system is not enough to improve socio-economic inclusion or civic participation. The Malawi case reveals that high levels of government coordination are needed to ensure that people realize the benefits of a digital ID system. Additionally, efforts must be made to protect systems from misuse to maintain public faith in the integrity of databases of sensitive information.

Special Considerations for Marginalized Groups

Generally, NDI's survey and focus group discussions revealed that the digital ID system had a net positive impact on the ease of the voter registration process in Malawi. BVR and the NRIS made it easier to change polling stations after moving and reduced voter fraud.[71] [72] No respondents in NDI's survey identified groups that found it easier or harder to vote after the introduction of the digital ID system.[73] However, when it comes to specific marginalized groups, research identified a number of shortcomings.[74]

Having to cross long distances to registration sites to register or renew ID cards poses barriers to the elderly and disabled, who may face difficulty reaching the site locations. Persons with albinism in Malawi who live far from registration sites may also be unable to travel far to obtain a national ID card, due to fear of being targeted for their appearance.[75] Officials from the Malawi Electoral Commission (MEC) made efforts to address geographic barriers to ID access during the initial rollout period through the use of mobile registration sites.[76] However, focus groups revealed that these efforts at inclusion may not have gone far enough: a lack of training in sign language for registration officials made it difficult for the Deaf community to register, and registration sites were often physically inaccessible.[77] Voter registration has long failed to accommodate the needs of persons with disabilities in Malawi, and those who have sensory or physical disabilities often need to rely on family members to assist them in the registration and voting process.[78] Due to the perceived lack of consultation between the government and disability rights organizations before, during, and after the initial registration rollout, and due to a lack of legislation in place to ensure persons with disabilities can register and vote, digitizing the voter registration system has failed to close this gap in Malawi.[79] [80]

A similar lack of consultation impacted other groups who could have benefited from inclusion from the outset of the design process. Focus group participants felt that the government did little to engage with LGBTQI+ communities ahead of NRIS implementation, which ultimately contributed to uncomfortable experiences for those who attempted to register. Transgender and gender non-conforming people struggled to prove their gender identity to officials, and were uncomfortable with the need to share additional gender identity information to register.[81] Many LGBTQI+ people left feeling that the registration process had been discriminatory, and similar reports of discrimination came from naturalized Malawian citizens whose parents had immigrated to the country.[82] A more inclusive design process would have made sure clear standards for proving identity were applied equally across all people, regardless of gender presentation or parents' immigration status.

Long-Term Sustainability

Almost every discussion of Malawi's NRIS, whether with marginalized people or in expert interviews, identified the cost of renewing ID cards as an inclusion issue.[83] [84] The first set of NRIS cards were set to expire in January 2021, making the window of time before renewal is required much shorter than that of a passport or driver's license.

While participants and respondents recognized the importance of renewing ID cards to remove ghost voters and streamline public social spending, the relatively high cost that individuals would need to shoulder to renew their cards was seen as prohibitive and exclusionary.[85] The relatively short period

for which Malawi's new national ID is valid, and the current cost associated with renewing the national ID, mean that when one's first identification card expires, those without the financial means to renew will be excluded from the voting process in future elections.[86] Respondents felt that no one should have to pay to renew their own citizenship, which is what the NRIS cards have come to represent.[87]

This challenge in Malawi underscores the importance of considerations of not only short-term deployment costs when designing a digital ID system for inclusion, but a plan for inclusively managing the long-term costs of a tech-empowered system in the future, lest the right to have a voice in government fall only to those who can afford the price tag.

Case Study: Data Privacy Concerns and Digital ID in Nigeria

Nigeria's move towards a national digital identification system began with creation of the National Identity Management Commission (NIMC) in 2007. NIMC issues the National Identity Number (NIN), a unique eleven-digit number assigned to each individual, as well as a national electronic identity card.[88]

A Complex Identification Ecosystem

The NIN was introduced to track fraud, support national security efforts, and assist the government in providing social services. However, experts argue that many of these aims have not been realized due to Nigeria's complex and duplicative identification regime: fourteen different government agencies have operated their own digital identity systems.[89] Respondents to an NDI survey from Nigeria noted the stress of having multiple IDs and wished for a more harmonious system.[90]

In addition to fragmentation, the identification ecosystem also operates under a weak data protection regime, in which citizens are often uninformed on data storage and usage. As a result, many Nigerians are concerned about the data collection, storage, and usage that occurs during the digital ID registration process. One respondent to NDI's survey described his perception of government motivations behind collecting personal data in Nigeria: "The idea of a multiple data collection in a period where the government is clamping down on those who speak out against irregularities in governance is worrisome for me. Why now? and What is the Data for? These questions have yet to be answered."[91] Interviews with civil society representatives reinforced fear and concern over the security of the data and potential abuse or misuse to crack down on social activists and political opponents.[92] Interviewees also noted that people are not informed on the use of their data, and many agents at enrollment centers are unable to explain how the data will be used, though this last claim was dismissed by government officials.[93]

Concerns over data collection can be compounded for vulnerable populations who may face additional threats from non-consensual data sharing and usage. A World Bank qualitative study on barriers to inclusion of women and marginalized communities in Nigeria's digital ID system notes that focus group participants "were reluctant to give personal information because they feared that their information would not be kept confidential and that it could be misused."[94] Building stronger data protection legislation and practices is vital to both ensure confidence and protect against harms in Nigeria's digital ID system.

Foreign Influence and Third-Party Data Sharing

In Nigeria's weak data protection context, concerns over data sharing without informed consent remain widespread, particularly when it involves sharing between government agencies and third-party companies. Research from The Engine Room revealed that government agencies in Nigeria sold datasets to financial institutions, telecommunications companies, and third-party marketers.[95] The Engine Room's report also noted concerns over the security of personally identifiable information (PII) as a result of the country's high rates of cybercrime. Non-consensual data sharing

reinforces perceptions of abuse and discourages individuals, especially those from marginalized populations, from participating in enjoying the benefits associated with a digital ID system.

In Nigeria, concerns over data-sharing are not just domestic. Mastercard's sponsorship of the initial rollout of the digital ID has led to concerns about corporate access to citizens' PII.[96] [97] The partnership with MasterCard raised concerns over who would collect and host records: the national government or an international company with fewer enforceable mechanisms for transparent and accountable data practices.[98] Transparent data flows are vital to ensure that the benefits of digital ID in Nigeria do not come at the price of surveillance capitalism. In Nigeria, civil society has played a key role in raising awareness and demanding greater transparency. Paradigm Initiative, a Nigerian digital rights group, raised awareness about potential foreign corporations gaining access to personal data, and promoted a digital rights and freedoms bill that was signed into law in April 2019.[99]

Focusing on Data Literacy

Government and civil society representatives agree that strong data protection laws and regulations are needed to bring transparency and confidence to digital ID data collection, usage, and storage in Nigeria. However, interviews with civil society representatives suggest that there has not been enough effort undertaken to talk about the benefits of digital ID in accessible ways; the conversation is in technical terms that prevent citizens from understanding the costs and benefits of digital ID. Laws and regulations should be paired with data literacy education campaigns to make citizens aware of their rights when it comes to data protection and privacy. Paradigm Initiative's public consultation on the draft 2020 Data Protection Bill is a blueprint for other civil society groups looking to create open spaces for discussion and hold governments accountable.[100]

Case Study: Voting Concerns and Distrust in Zimbabwe

In the lead up to Zimbabwe's 2018 elections, the country introduced a voluntary biometric voter registration (BVR) process to improve public service distribution and to address administrative problems of ghost voters and voter duplication.[101] [102] In preparation for the BVR rollout, the government encouraged citizens to minimize registration problems by ensuring they had a legal ID, and that their national ID cards were updated to the new biometric version first introduced in 2010 as part of the Zimbabwe Population Registration System (ZPRS).[103]

Designed as a replacement for the previous metal-based cards, the new plastic cards display a person's national identity number, name, date of birth, village of origin, place of birth, card issuance date, and the holder's fingerprint and signature.[104] In addition, the ZPRS database contains additional details not printed on the card, including birth certificate information and the ID numbers of the holder's parents or legal guardians.[105]

A Non-Inclusive Registration Process

As efforts intensified to register potential voters for a national ID in advance of the BVR, concerns emerged about a lack of information-sharing regarding changes to the national ID process. Respondents to an NDI survey reported that the general population had little knowledge of the government's intentions or purpose for collecting biometric data due to a lack of public consultation during the development of the systems and the absence of a large-scale initiative to raise public awareness.[106] In separate focus group research conducted by The Engine Room, participants noted that the government had done a particularly poor job reaching out to members of marginalized groups, such as farmers, street vendors, rural residents, and women to explain the benefits of the new digital ID system.[107]

Some groups face unique additional challenges when registering for a digital ID in Zimbabwe. Although existing identification documents are required to register, some individuals, such as members of rural communities where home births are common, may never have been issued a birth certificate, further complicating their ability to prove their identity. Similarly, orphans and members of conflict-affected communities such as the Gukurahundi have struggled to identify themselves because they lack access to their parents' documents.[108] Zimbabwe's transgender community faces even higher barriers to obtaining a new digital ID, as officials from the Registrar General's office have harassed individuals whose gender presentation does not match what is listed on their birth certificates.[109]

Protecting Confidential Data

The lack of transparency and public outreach around the deployment of biometric-based ID and voter registration systems has also sparked fears that the data provided by an individual to the government may be used negatively against them. Following the 2018 election, observers heard reports of "numerous incidents of ruling party or government officials demanding to see citizens' voter registration slips and saying that the new voter registration system would allow them to know how the person voted."[110] Fears that an individual's vote will be shared can further intimidate those

who are dependent on government subsidies or assistance, especially if the aid is either overtly or implied to be conditional upon casting a vote for a certain party or candidate. In 2018 for example, community development projects were commonly conflated with campaign events promoting ZANU-PF candidates.[111]

Zimbabwean citizens and international watchdog organizations have raised concerns about the ways in which the government collects, manages, and shares data. NDI survey respondents noted that a central concern is where personal data will go and who will have access to it. The Engine Room reported fears from sex workers, members of the LGBTQI+ community, and those living with HIV/AIDS that health data tied to their national identity card could be shared across government agencies to NGOs and churches that would discriminate against them for their HIV positive status.[112] Some anti-government activists have expressed reluctance to leave their information on file with the Registrar General's office, due to fears of retaliation if it were to be shared with the ruling party.[113] A respondent to an NDI survey noted that "there are fears that the data privacy is not secure and there are reported high levels of corruption within the registry department."[114]

Next Steps

As Zimbabwe continues its efforts to register citizens into biometric-based systems, considerations such as data security, privacy, inclusion, and interoperability should be taken into account. Beyond the ZPRS, several other biometric based systems have been rolled out, including those intended to purge ghost workers from the civil service, a system to identify and collect tax from street vendors, and a pilot funded in part by the World Food Program to facilitate cash transfers.[115] [116] [117] With the ZEC, Registrar General, and others collecting vast quantities of personal data and allowing third parties to process it digitally, establishing standards for the protection of that data is important.

Zimbabwe's 2019 Cybersecurity and Data Protection Bill is aimed at protecting the right to privacy and personal data, and provides for the collection, use and storage of personal data by both state and private bodies.[118] Although the bill prohibits the processing of sensitive information (including biometric data), unless written consent by the data subject is provided, it makes a number of exceptions that may potentially override that consent without a user's knowledge, such as the "prevention of imminent danger", compliance with national security laws, or even for "purposes of scientific research."[119] However, due to citizens' lack of trust of the government, the bill may not fully provide the protection needed.[120] MISA Zimbabwe, a freedom of expression organization, published an analysis of the bill upon its release, advocating for a number of steps to be taken, including: ensuring the bill conforms with international legal frameworks such as the African Declaration on Internet Rights and Freedoms; accepting input from key stakeholders and the general public; and ensuring that the application of national security provisions mentioned in the bill are in line with Zimbabwe's human rights framework in the Constitution.[121]

References

[1] World Bank Group. ID4D Data: Global Identification Challenge by the Numbers. https://id4d.worldbank.org/global-dataset
[2] United Nations. Sustainable Development Goals, Goal 16: Peace, justice and strong institutions. https://www.un.org/sustainabledevelopment/peace-justice/
[3] World Bank Group. (2018). G20 Digital Identity Onboarding. https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf
[4] UN General Assembly. (2019, October 11). Extreme poverty and human rights. https://undocs.org/A/74/493
[5] Center for Human Rights and Global Justice. (2021). Chased Away and Left to Die. https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf
[6] International Monetary Fund. (2021). The Role of E-Government in Promoting Foreign Direct Investment Inflows. https://www.imf.org/en/Publications/WP/Issues/2021/01/15/The-Role-of-E-Government-in-Promoting-Foreign-Direct-Investment-Inflows-49981
[7] World Bank Group. (2019). Achieving Universal Access to ID: Gender-based Legal Barriers Against Women and Good Practice Reforms. https://openknowledge.worldbank.org/handle/10986/32474
[8] McKinsey Global Institute. (2019, April). Digital Identification: A key to inclusive growth. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx
[9] United Nations. Legal Identity Agenda. https://unstats.un.org/legal-identity-agenda/
[10] World Bank Group. Identification for Development. https://id4d.worldbank.org/
[11] World Bank Group, ID4D. (2019, October). Digital ID and the Data Protection Challenge. https://documents1.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf
[12] UN General Assembly. (2019, October 11). Extreme poverty and human rights. https://undocs.org/A/74/493
[13] UN General Assembly. (2019, October 11). Extreme poverty and human rights. https://undocs.org/A/74/493
[14] GSMA. Digital Identity Programme. https://www.gsma.com/mobilefordevelopment/digital-identity/
[15] Anderson T., & Odhiambo F. (2020, October 5). Partner Spotlight: Paradigm Initiative's Vision for Ensuring Good ID and Data Protection in Nigeria. Omidyar Network. https://omidyar.com/partner-spotlight-paradigm-initiatives-vision-for-ensuring-good-id-and-data-protection-in-nigeria/
[16] The Engine Room. (2020, January). Understanding the Lived Effects of Digital ID A Multi-Country Study. https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf
[17] Access Now. #WhyID. https://www.accessnow.org/whyid/#current-problems
[18] Center for Global Development. Biometrics and the ID Revolution. https://www.cgdev.org/topics/technology/biometrics
[19] More information on National Democratic Institute's work in Malawi, Nigeria, Zimbabwe, please see: https://www.ndi.org/sub-saharan-africa
[20] Access Now. (2018, May). National Digital Identity Programmes: What's Next? https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf
[21] Macdonald, A. (2021, February 2). Nigeria's move to link digital identity numbers to SIM cards sparks lawsuit. BiometricUpdate. https://www.biometricupdate.com/202102/nigerias-move-to-link-digital-identity-numbers-to-sim-cards-sparks-lawsuit
[22] Chandran, R. (2021, April 15). Fears of vaccine exclusion as India uses digital ID, facial recognition. Reuters. https://www.reuters.com/article/india-health-coronavirus/fears-of-vaccine-exclusion-as-india-uses-digital-id-facial-recognition-idUSL8N2M11TH
[23] National Democratic Institute. (2021, March). Digital ID Survey.
[24] Maier, A. (2014, Winter). Designing With, Not For. Civic Quarterly. https://www.civicquarterly.com/article/designing-with-not-for
[25] World Wide Web Foundation. (2019, August 28). Digital ID tech must be transparent if it is to work for citizens. https://webfoundation.org/2019/08/digital-id-tech-must-be-transparent-if-it-is-to-work-for-citizens/
[26] National Democratic Institute. (2021, March). Digital ID Survey.
[27] National Democratic Institute. (2021, March). Digital ID Survey.
[28] National Democratic Institute. (2021). Interviews with various digital rights experts.
[29] Ordinario, C. (2021, June 3). Mapa: PSA taps malls for National ID registration. BusinessMirror. https://businessmirror.com.ph/2021/06/03/mapa-psa-taps-malls-for-national-id-registration/
[30] Share, F. (2017, August 30). RG's Office rolls out mobile reg •Nationwide programme to run for 3 months •Metal IDs to be phased out. 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/
[31] Juncosa, M.L., & Shapiro, N., & Turn, R. (1975). Privacy and Security in Centralized vs. Decentralized Databank Systems. Rand Corporation. https://www.rand.org/pubs/papers/P5346.html
[32] Access Now. (2018, November). Creating a Data Protection Framework: a Do's and Don't Guide for Lawmakers. https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf
[33] Funk, A., & Shahbaz, A. The Pandemic's Digital Shadow. Freedom House. https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow
[34] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.
[35] Crossroads' Global Hand. Microsoft partners with aid agencies to provide essential technology. https://www.globalhand.org/en/browse/partnering/6/success+story/document/20808
[36] MasterCard. (2013, May 8). Press Release: MasterCard to Power Nigerian Identity Card Program: 13 Million Cards to be issued first, in largest card rollout of its kind in Africa. https://newsroom.mastercard.com/press-releases/mastercard-to-power-nigerian-identity-card-program/

[37] 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/
[38] Couldry, N., & Mejias, U. (2018, September 2). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. Sage Journals. https://journals.sagepub.com/doi/abs/10.1177/1527476418796632?journalCode=tvna&
[39] National Democratic Institute. (2021, March). Digital ID Survey.
[40] Geiser, U. (2021, March 7). Digital identity scheme shot down by voters over data privacy concerns. Swiss Info. https://www.swissinfo.ch/eng/digital-identity-scheme-faces-scepticism-around-data-privacy/46399636
[41] Crider, C., & Fitzgerald, M. (2021, March 30). We've won our lawsuit over Matt Hancock's £23m NHS data deal with Palantir. openDemocracy. https://www.opendemocracy.net/en/ournhs/weve-won-our-lawsuit-over-matt-hancocks-23m-nhs-data-deal-with-palantir/
[42] USAID. Identity in a Digital Age: Infrastructure for Inclusive Development. https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf
[43] International IDEA. If the EMB Uses Technology to Collect Voter Registration Data, Is Biometric Data Captured and Used During Registration?. https://www.idea.int/data-tools/question-view/738
[44] Wolf, P. (2017). Introducing Biometric Technology in Elections. International IDEA. https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf
[45] Diofasi, A., & Gelb, A. (2016, August 17). Biometric Elections in Poor Countries: Wasteful or a Worthwhile Investment? - Working Paper 435. Center for Global Development. https://www.cgdev.org/publication/biometric-elections-poor-countries-wasteful-or-worthwhile-investment
[46] Clark, J., & Gelb, A. (2013, January). Identification for Development: The Biometrics Revolution - Working Paper 315. Center for Global Development. https://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf
[47] Macdonald, A. (2021, January 25). Nigerians don't need national digital ID for voter enrollment, EC says. BiometricUpdate. https://www.biometricupdate.com/202101/nigerians-dont-need-national-digital-id-for-voter-enrollment-ec-says
[48] Wolf, P. (2017). Introducing Biometric Technology in Elections. International IDEA. https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf
[49] World Bank Group, ID4D. (2020). Creating Disability Inclusive ID Systems. https://documents1.worldbank.org/curated/en/967741605683569399/pdf/Creating-Disability-Inclusive-ID-Systems.pdf
[50] USAID. Identity in a Digital Age: Infrastructure for Inclusive Development. https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf
[51] USAID. Identity in a Digital Age: Infrastructure for Inclusive Development. https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf
[52] 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/
[53] International Republican Institute (IRI) and National Democratic Institute (NDI) Zimbabwe International Election Observation Mission (ZIEOM) (2018, August 1). Preliminary Statement. https://www.ndi.org/sites/default/files/8-1-18-ZIEOM%20Final%20Statement%20w%3A%20Delegation-cs.pdf
[54] Diofasi, A., & Gelb, A. (2016, August 17). Biometric Elections in Poor Countries: Wasteful or a Worthwhile Investment? - Working Paper 435. Center for Global Development. https://www.cgdev.org/publication/biometric-elections-poor-countries-wasteful-or-worthwhile-investment
[55] Diofasi, A., & Gelb, A. (2016, August 17). Biometric Elections in Poor Countries: Wasteful or a Worthwhile Investment? - Working Paper 435. Center for Global Development. https://www.cgdev.org/publication/biometric-elections-poor-countries-wasteful-or-worthwhile-investment
[56] The Engine Room. (2020, January). Understanding the Lived Effects of Digital ID A Multi-Country Study. https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf
[57] 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
[58] van den Staak, S., & Wolf, P. (2019). Cybersecurity in Elections Models of Interagency Collaboration. International IDEA. https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf
[59] Malik, T. (2018). A Quick Roll-out Strategy for eID Projects in fulfilment of SDG 16.9: A Case Study of Malawi. UNDP. https://www.id4africa.com/2018_event/Presentations/PS3/1-3-6_UNDP_Malawi_TariqMalik.pdf
[60] Malik, T. (2018). A Quick Roll-out Strategy for eID Projects in fulfilment of SDG 16.9: A Case Study of Malawi. UNDP. https://www.id4africa.com/2018_event/Presentations/PS3/1-3-6_UNDP_Malawi_TariqMalik.pdf
[61] National Democratic Institute. (2020-21). Internal interview with digital rights expert.
[62] National Democratic Institute. (2020-21). Internal Malawi focus group.
[63] National Democratic Institute. (2020-21). Internal interview with various digital rights experts.
[64] National Democratic Institute. (2021, March). Digital ID Survey.
[65] National Democratic Institute. (2021, March). Digital ID Survey.
[66] National Democratic Institute. (2021). Internal interview with Vincent Kumwenda.
[67] European Union, Election Observation Mission. (2014, May 20). Final Report: Tripartite Elections: Presidential, Parliamentary and Local Council. https://www.eisa.org/pdf/mal2014eu.pdf
[68] Tyburski, L. (2019, November 1). Malawi's Election Was Not Stolen With White-Out. Foreign Policy. https://foreignpolicy.com/2019/11/01/malawis-election-was-not-stolen-with-white-out/
[69] National Democratic Institute. (2021, March). Digital ID Survey.
[70] National Democratic Institute. (2020-21). Internal interview with digital rights expert.
[71] National Democratic Institute. (2020-21). Internal Malawi focus group.
[72] National Democratic Institute. (2021, March). Digital ID Survey.
[73] National Democratic Institute. (2021, March). Digital ID Survey.
[74] National Democratic Institute. (2020-21). Internal interview with digital rights expert.
[75] National Democratic Institute. (2020-21). Internal interview with digital rights expert.
[76] National Democratic Institute. (2020-21). Internal interview with digital rights expert.

[77] National Democratic Institute. (2020-21). Internal Malawi focus group.
[78] Masina, L. (2014, April 15). Malawian Blind Voters Push for Tactile Ballots. VOA Africa. https://www.voanews.com/africa/malawian-blind-voters-push-tactile-ballots
[79] National Democratic Institute. (2020-21). Internal Malawi focus group.
[80] National Democratic Institute. (2020-21). Internal interview with digital rights expert.
[81] National Democratic Institute. (2020-21). Internal Malawi focus group.
[82] National Democratic Institute. (2020-21). Internal interview with Vincent Kumwenda.
[83] National Democratic Institute. (2020-21). Internal Malawi focus group.
[84] National Democratic Institute. (2020-21). Internal interview with various digital rights experts.
[85] National Democratic Institute. (2020-21). Internal Malawi focus group.
[86] National Democratic Institute. (2020-21). Internal Malawi focus group.
[87] National Democratic Institute. (2020-21). Internal Malawi focus group.
[88] Centre for Internet and Society. (2020, November 3). Mapping Digital Identity Systems: Nigeria. https://digitalid.design/research-maps/nigeria.html
[89] Government of Nigeria. (2020, August 13). Citizen Data Management And Harmonization Report. Medium. https://theasovilla.medium.com/citizen-data-management-and-harmonization-report-1e0fd4d7444a
[90] National Democratic Institute. (2021, March). Digital ID Survey.
[91] National Democratic Institute. (2021, March). Digital ID Survey.
[92] National Democratic Institute. (2020-21). Internal interview with digital rights expert.
[93] National Democratic Institute. (2020-21). Internal interview with digital rights expert.
[94] World Bank Group. (2021). Barriers to the Inclusion of Women and Marginalized Groups in Nigeria's ID System. https://documents1.worldbank.org/curated/en/881401618990982108/pdf/Barriers-to-the-Inclusion-of-Women-and-Marginalized-Groups-in-Nigeria-s-ID-System-Findings-and-Solutions-from-an-In-Depth-Qualitative-Study.pdf
[95] The Engine Room. (2019). Digital ID in Nigeria: A case study. https://digitalid.theengineroom.org/assets/pdfs/[English]%20Nigeria%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf
[96] Court, A. (2014, September 25). Branding Nigeria: MasterCard-backed I.D. is also a debit card and a passport. CNN. https://www.cnn.com/2014/09/25/business/branding-nigeria-mastercard-backed-i-d-/index.html
[97] Mastercard. (2014, August 28). Press Release: MasterCard-branded National eID Card Launched in Nigeria. https://newsroom.mastercard.com/mea/press-releases/mastercard-branded-national-eid-card-launched-nigeria/
[98] O'Grady, S. (2014, September 3). Nigeria's Orwellian Biometric ID Is Brought to You by MasterCard. Foreign Policy. https://foreignpolicy.com/2014/09/03/nigerias-orwellian-biometric-id-is-brought-to-you-by-mastercard/
[99] Adegoke, A., & Ilori, T. (2019, August 3). Digital Rights and Freedom Bill Archives: The Leap and the Hurdles. Paradigm. https://paradigmhq.org/the-digital-rights-and-freedom-bill-the-leap-and-the-hurdles/
[100] Anderson T., & Odhiambo F. (2020, October 5). Partner Spotlight: Paradigm Initiative's Vision for Ensuring Good ID and Data Protection in Nigeria. Omidyar Network. https://omidyar.com/partner-spotlight-paradigm-initiatives-vision-for-ensuring-good-id-and-data-protection-in-nigeria/
[101] National Democratic Institute. (2020-21). Internal interview with Chenai Chair.
[102] Le Roux, J. (2018, July 16). Zimbabwean voters roll haunted by doppelgangers, ghosts. News24. https://www.news24.com/Africa/Zimbabwe/zimbabwean-voters-roll-haunted-by-doppelgangers-ghosts20180716
[103] 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/
[104] ICAO. (2012). The Zimbabwean Situation. https://www.icao.int/Meetings/mrtd-Zimbabwe2012/Documents/6-Mudede_Machiri_Zimbabwe-Situation.pdf
[105] Zimbabwe, Department of the Registrar General. The National Registration. http://www.rg.gov.zw/index.php/services/national-registration
[106] National Democratic Institute. (2021, March). Digital ID Survey.
[107] The Engine Room. (2019). Digital ID in Zimbabwe: A case study. https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf
[108] National Democratic Institute. (2020-21). Internal interview with digital rights expert.
[109] The Engine Room (2019) Digital ID in Zimbabwe: A case study. https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf
[110] International Republican Institute (IRI) and National Democratic Institute (NDI) Zimbabwe International Election Observation Mission (ZIEOM) (2018, August 1). Preliminary Statement. https://www.ndi.org/sites/default/files/8-1-18-ZIEOM%20Final%20Statement%20w%3A%20Delegation-cs.pdf
[111] International Republican Institute (IRI) and National Democratic Institute (NDI) Zimbabwe International Election Observation Mission (ZIEOM) (2018, August 1). Preliminary Statement. https://www.ndi.org/sites/default/files/8-1-18-ZIEOM%20Final%20Statement%20w%3A%20Delegation-cs.pdf
[112] The Engine Room. (2019). Digital ID in Zimbabwe: A case study. https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf
[113] The Engine Room. (2019). Digital ID in Zimbabwe: A case study. https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf
[114] National Democratic Institute. (2021, March). Digital ID Survey.
[115] Chindaro, S. (2018, December 10). Using Biometrics to eliminate "Ghost Workers" in the Civil Service in Zimbabwe. http://drsamuelchindaro.blogspot.com/2018/12/using-biometrics-to-eliminate-ghost.htm

[116] The Herald (2016) SMEs chamber launches Biometric Database**.** https://www.herald.co.zw/smes-chamber-launches-biometric-database/
[117] The Engine Room. (2019). Digital ID in Zimbabwe: A case study. https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf
[118] Veritas. (2019). Cyber Security and Data Protection. http://veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf
[119] Veritas. (2019). Cyber Security and Data Protection. http://veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf
[120] MISA-Zimbabwe. MISA-Zimbabwe Commentary: Cybersecurity and Data Protection Bill HB 18 of 2019. https://zimbabwe.misa.org/2020/05/19/cybersecurity-and-data-protection-bill-entrenches-surveillance-an-analysis/
[121] MISA-Zimbabwe. MISA-Zimbabwe Commentary: Cybersecurity and Data Protection Bill HB 18 of 2019. https://zimbabwe.misa.org/2020/05/19/cybersecurity-and-data-protection-bill-entrenches-surveillance-an-analysis/