Understanding
the Lived Effects
of Digital ID
A Multi-Country Study

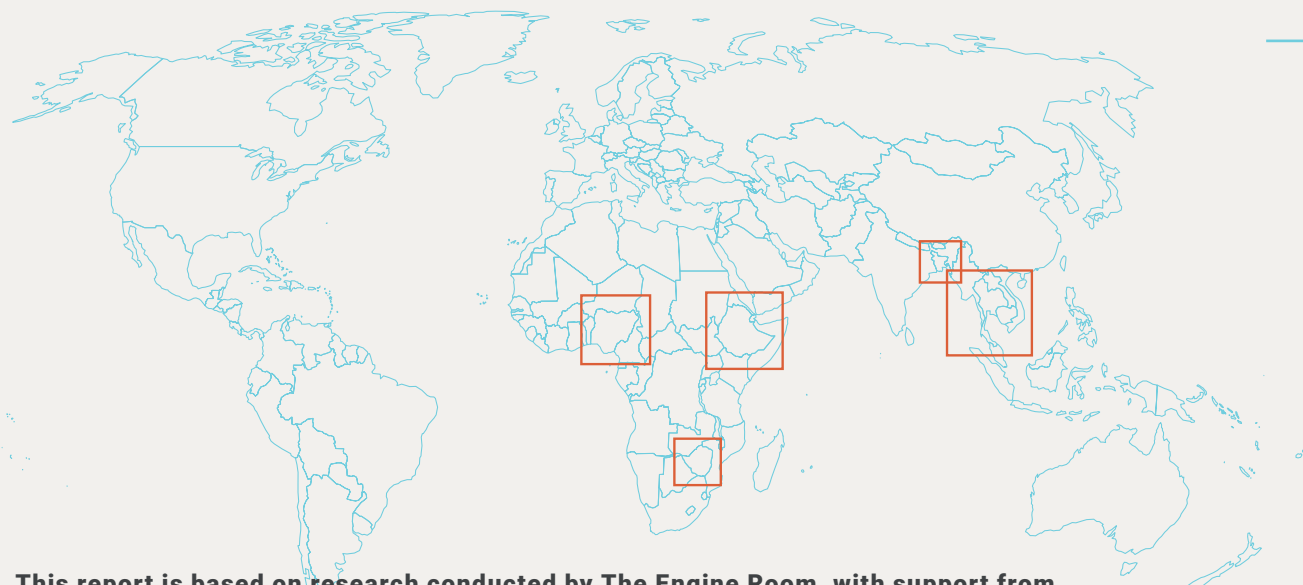JANUARY 2020

THE ENGINE ROOM

Understanding the Lived Effects of Digital ID

A Multi-Country Study

Table of Contents

Executive Summary

Situated at the intersection of numerous rights, digital ID systems affect people's daily lives for better or worse. As these systems flourish, most research and reporting focuses on technological aspects, implementation benchmarks, and policies and legislation, failing to capture the experiences of diverse populations using digital ID. Through locally led research, this report documents many of the lived effects of digital ID systems from design to roll-out among mostly marginalised communities in Bangladesh, Ethiopia, Nigeria, Zimbabwe and Thailand.

Our research surfaced key tensions within digital ID ecosystems, including empowerment vs. surveillance, data sharing vs. data privacy, and benefits for some vs. harm to others. Institutions developing and implementing digital ID systems often prioritise their own needs (e.g., efficiency in benefits distribution, national security, financial goals) over a variety of human rights, such as the right to privacy and freedom of expression.

While digital ID systems do provide important benefits, such as access to services, our key findings reflect challenges faced by communities in every site we studied. They include:

- **Low levels of public and civil society involvement**
- **Barriers to registration and use**
- **Lack of informed consent**

- **Concerns about data use and protection**
- **Lack of shared language on digital ID**
- **Failure to consider local context**

Through this report, we aim to amplify in-country voices that are often left out of regional and global discussions on digital ID and to encourage more interaction between decision-makers and people, especially communities that can benefit most from, but also face the biggest risks in relation to, digital ID infrastructure, policies and protocols.

We conducted this research as a nonprofit organisation seeking to support civil society in working toward social justice. This research is, for us, a step towards more informed and evidence-based advocacy; already, researchers involved have used their findings to engage in advocacy in their respective contexts. We hope that findings here will also be used by others in pushing for more context-respecting digital ID systems and to inspire more context-respecting research of sociotechnical systems.

A woman taking part in the process of making voter and national ID cards in Bangladesh

Introduction

The World Bank estimates that one billion people around the world, most of them living in Africa and Asia, do not have documentation that proves their legal identities.[1]

Such documentation – a birth certificate, passport, driver's license or refugee identity certificate – is often required for opening a bank account, voting, getting a job, accessing education or healthcare or even buying a SIM card for a mobile phone.

Volunteer sanitation workers at work in refugee camps in Ethiopia

This so-called 'identification gap' represents a growing concern for governments, aid agencies and humanitarian organisations working to sustain systems of education, healthcare, financial and social services for large populations. There is a strong and understandable impetus to be able to identify and count all of the people served by these entities to better understand their needs, and the digital era presents a unique opportunity to do just that.

The drive to close the 'identification gap' was articulated with Target 16.9 of the United Nations Sustainable Development Goals, which states, "By 2030, provide legal identity for all, including birth registration".[2] While there is no requirement that legal identities be digital, a growing number of governments and multilateral organisations are now using digital technology to provide identification. But digitisation is no small feat, and there are many approaches that institutions can take to achieve this goal. Many institutions are taking the step of gathering biometric data – that is, unique measurements taken from people's bodies – as part of those digital ID systems. As discussed in this report, biometric data has particular, long-lasting privacy concerns for individuals, as the data is immutable and forever connected to a person's body.

The design and deployment of each system for identity digitisation can have unique benefits and consequences for the populations it is meant to serve. Today, hundreds of millions of

people around the world are now navigating complex digital ID infrastructure in order to gain or retain access to basic government and humanitarian services.

As these systems proliferate, concerns about their negative effects on individuals and vulnerable communities have emerged.[3] How does a single digital ID system affect various populations differently? Our research explores this question by assessing digital ID as a sociotechnical system and identifying some of the consequences that it can carry, alongside its benefits, in five different sites around the world.

In particular, we endeavor to examine the friction that occurs between a person's legal identity and the many other identities they can possess. How do digital ID systems affect the range of identities that shape people's lives, such as race and ethnicity, gender identity, sexuality, religion, caste, economic class and ability? When systems fail to serve people, how does this failure affect their agency, dignity or ability to exercise their human rights?

Through field research involving key informant interviews and focus groups, we pursued answers to these questions by speaking with more than one hundred individuals who have already obtained or are expected to obtain digital ID cards or credentials in Nigeria, Zimbabwe, Thailand and in refugee camps in Bangladesh and Ethiopia.

In response to the increased push for global norms and scaling of systems, we sought to explore the ways in which unique local contextual realities can impact the effectiveness of digital ID systems. Our distributed team included seven embedded researchers hailing from and living in these five countries. This gave us a unique ability to prioritise contextual knowledge, participatory methods and a respectful, culturally fluent approach to gaining insights. We indeed found that context-specific approaches to identification can be the most effective, even if not the most resource efficient. We hope that our findings might shift the way the field considers (and conducts inquiries into) digital ID.

This global report covers cross-cutting themes observed in our five case sites and is followed by case studies from each site, which can be read along with the report for further details or used independently in local communities for advocacy. We hope this report will help civil society, researchers, journalists, technologists, humanitarian organisations and governments understand the experiences of people living with digital ID or in regions where digital ID systems are planned and incorporate lessons from those experiences into their work.

Scope and objectives

For the purposes of this project, we defined 'digital ID' as systems using digital technology to identify and verify individuals for a variety of purposes ranging from public service delivery and aid distribution to national security. Often, but not always, these systems use biometric data. We focused on experiences with foundational IDs (general identification for public administration) in national contexts and functional IDs (identification for a specific purpose such as access to social services) in refugee camps.[4] Notably, local definitions and understandings of digital ID vary, an issue which is addressed in the findings.

We began with desk research in late 2018 to determine which systems to examine, and we selected sites based on the following broad criteria:

- **The ability for comparison across sites, where sensible**
- **Markers of potential trends in digital identity**
- **Contextual knowledge within The Engine Room**
- **Relative freedom of civil society to work on related issues**
- **Existence of digital ID systems at a stage where research of this kind could be helpful**

Because we aimed to ensure that our work supported the work and growth of in-country and regional civil society, we did not focus on countries with thriving advocacy on digital ID, such as Kenya or India. Given these criteria, we selected the following systems:

- UNHCR's digital ID systems in use with the Rohingya Muslim refugee population in Bangladesh and in refugee camps in Ethiopia
- Nigeria's national ID system led by the National Identity Management Commission, which will merge multiple ID systems into one
- Zimbabwe's upcoming national ID system, which began with support from a Chinese company, and the country's Biometric Voter Registration managed by the Zimbabwe Electoral Commission
- Thailand's upcoming digital ID system led by the Electronic Transactions Development Agency, although due to the system's slow progress, we broadened our focus to various Bureau of Registration Administration-led ID systems for marginalised populations, such as an ID system for migrant labourers known as the 'pink card'

Limitations

Security, logistical and time constraints meant that researchers were unable to interview some of the vulnerable groups they had initially identified. This ranged from remote rural communities in many sites to Rohingya people still living in Myanmar. Additionally, there were government and humanitarian representatives who did not respond or who declined to provide an interview.

We did not seek to study the experiences of representative samples of each population. Rather, we aimed to understand the lived experiences of individuals, placing special emphasis on those who have experienced disadvantages linked to their unique identity characteristics or life experiences. 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.

Finally, some systems were further developed than others during our research phase because implementing institutions did not keep to their original timelines or experienced delays during roll-out. As a consequence, we adjusted our research focus to explore experiences with other ID systems in the selected locations and/or with particular communities. For example, we narrowed our focus to specific vulnerable communities in Thailand. All considered, our research took place over a relatively short period of time (from February to April), and there remains a need for research on longer-term consequences in local contexts.
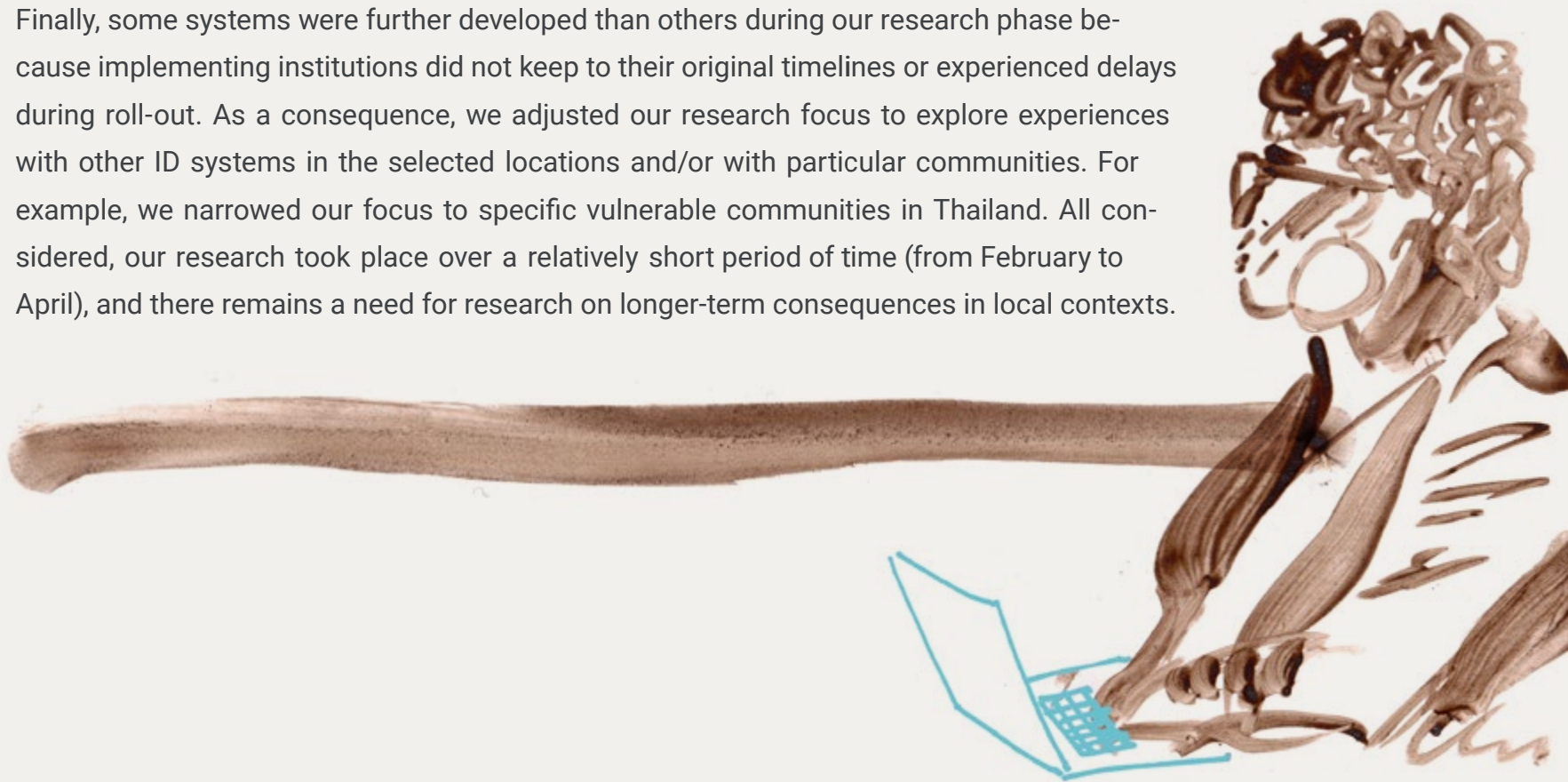
Findings

Introduction to system contexts

Bangladesh: Digital ID for Rohingya refugees in Cox's Bazar

The United Nations High Commissioner for Refugees (UNHCR) provides aid in the Cox's Bazar district of Bangladesh to Rohingya refugees who, in 2016 and 2017, fled extreme targeted violence carried out against them with genocidal intent[5] in Myanmar. With 600,000 refugees, the settlement of Kutupalong, one of two in the district, is the largest in the world.[6] In mid-2018 UNHCR and the Government of Bangladesh launched an identity verification exercise "for the purposes of protection, identity management, documentation, provision of assistance, population statistics and ultimately solutions for an estimated 900,000 refugees".[7]

The verification process involves the collection of three types of biometric data – face photographs, 10 fingerprints and two iris scans – for individuals age 13 and above. At the end

Landscape of a Rohingya refugee camp in Bangladesh

of the process, individuals receive identification cards. According to UNHCR, these cards — locally referred to as 'smart cards' — are the first IDs many Rohingya have ever obtained.[8] There has been significant controversy over these IDs, however.
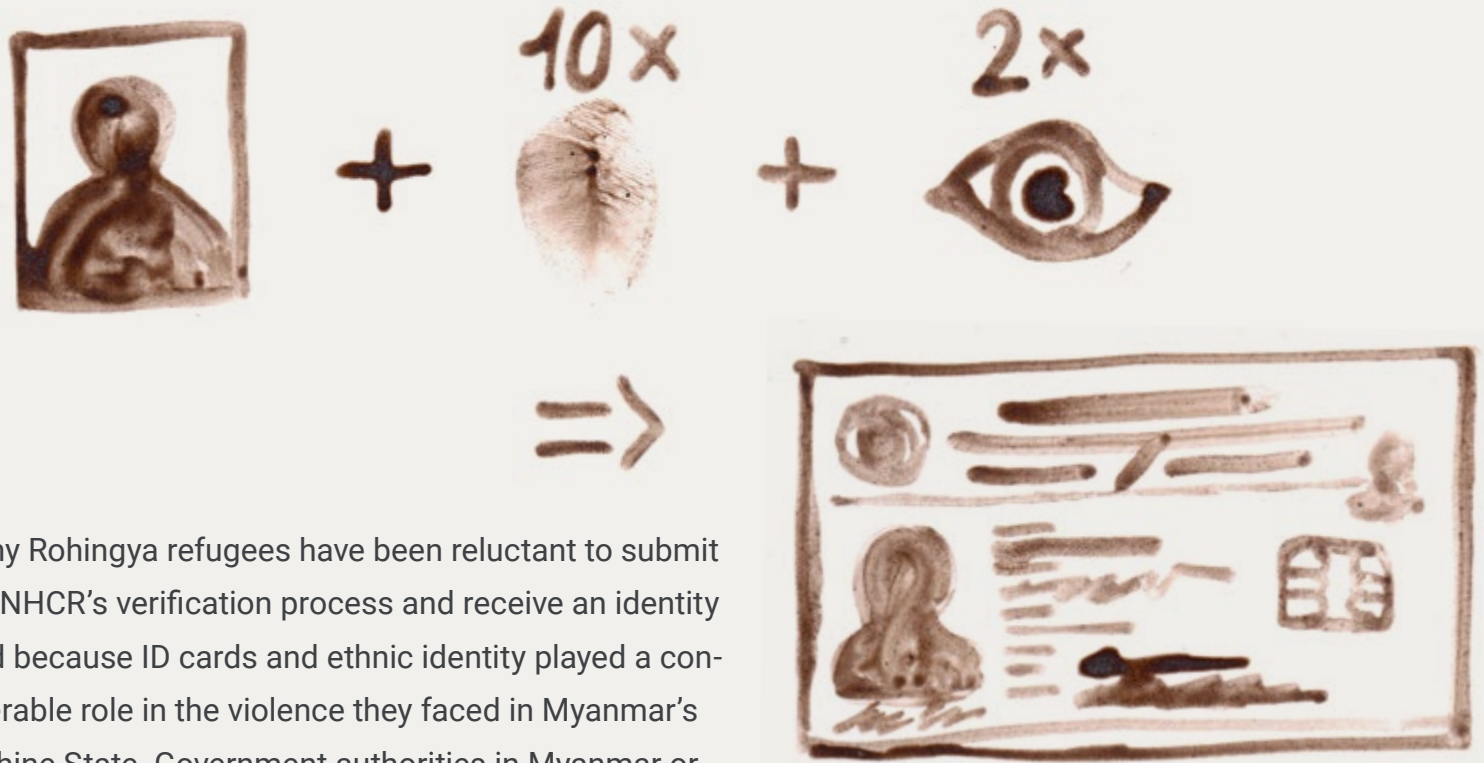
Many Rohingya refugees have been reluctant to submit to UNHCR's verification process and receive an identity card because ID cards and ethnic identity played a considerable role in the violence they faced in Myanmar's Rakhine State. Government authorities in Myanmar ordered Rohingya Muslims to accept National Verification Cards that deny their citizenship,[9] marking one of the many discriminatory policies the ethnic minority group has faced in Myanmar since the 1970s. The Myanmar government does not recognize the Rohingya as an ethnic people of Myanmar (though it officially recognises several other groups) and many are not granted citizenship despite being born in the country.

As violence escalated in 2016, displacing people, Rohingya people rejected the National Verification Cards (NVC), which they termed 'genocide cards'.[10] Fortify Rights reported that some Rohingya people were forced to accept the NVC cards at gunpoint.[11] In the months that followed, Myanmar military violence, movement restrictions, forced displacement and internment camps led hundreds of thousands of Rohingya Muslims to flee Myanmar for Bangladesh.[12]

Following this influx of people, the Bangladeshi government worked with UNHCR to provide shelter and humanitarian assistance. According to the Refugee and Repatriation Relief Commissioner (RRRC) of the Government of Bangladesh – the government official responsible for the Bangladeshi government's response to the Rohingya refugees – decisions about the framework of the digital ID system and the information collected were made jointly with UNHCR. In an interview with our researcher, the Commissioner also reported that the purposes of the card are to preserve individual identity, access aid, prevent duplication in the aid distribution process, and enable refugees to return to their home villages with proof of vital information such as their ancestry, family information, and employment.

On the latter point, UNHCR claims that the verification process and resulting smart card "will help preserve [refugees'] right to voluntarily return home, if and when they decide that the conditions are right to do so."[13] But on the two occasions Bangladeshi officials attempted to repatriate small groups of Rohingya refugees on a voluntary basis, in November 2018 and August 2019, none chose to return.[14]

On November 26, 2018, Rohingya Muslims began a protest and work strike in Cox's Bazar, demanding that UNHCR and the Government of Bangladesh add their ethnicity to smart cards.[15]

Two young refugee girls carry water to their camp in Ethiopia

This action led to deeper conversations between Rohingya leaders, UNHCR and the RRRC, and many refugee community leaders agreed to encourage people to register. As of October 2019, more than 762,000 Rohingya refugees had been registered and provided with identity documents as part of UNHCR's joint verification exercise with the Bangladeshi government.[16]

Following peaceful protests by Rohingya activists in August 2019, the Bangladeshi government ordered telecommunications companies to block all mobile phone access to the camps in Cox's Bazar.[17] Lack of formal ID cards has been cited by Mustafa Jabbar, Bangladesh's minister of telecommunications,[18] as one reason behind this denial of access. Within Bangladesh, national ID cards with biometric data have been required to purchase SIM cards on the grounds of national security since late 2015,[19] but it seems that many have purchased SIM cards on the black market, i.e., without IDs.[20]

Ethiopia: Digital ID for refugees

Ethiopia hosts more than 900,000[21] refugees, most of whom came from Eritrea, Somalia, Sudan, South Sudan and Yemen due to conflicts, wars and rights violations. Despite its own history of conflict, political upheaval, poverty and drought, Ethiopia is home to the second largest refugee population in Africa (Uganda being the first).[22] An asylum country since the 1990s,[23] the government hosts people in need with the support of international agencies such as the United Nations High Commissioner for Refugees (UNHCR).

Through the current verification system, UNHCR captures comprehensive information (e.g., skill set, in-depth education details, family members in other countries) plus biometric data

of a photograph, 10 fingerprints and, for individuals age five and up, an iris scan. An ID card is issued by the Ethiopian government's Agency for Refugee and Returnee Affairs (ARRA) and UNHCR. The UNHCR Registration Official in Addis Ababa told us that approximately 500,000 had been registered at the time of our research in April 2019.

Through the use of digital ID, UNHCR aims to increase access to services and opportunities such as child protection,[24] reunification and education.[25] As one UNHCR informant explained,

> The new Comprehensive Refugee Response Framework policy that was passed puts to use the detailed information you capture. It helps to know the work experience of refugees; for instance, if companies want to hire or if there are employment needs for the industrial parks, it is useful to know who has experience with computers and other skills. You can say the main use is to know the potential in the refugee population.

Additionally, comprehensive registration with biometrics aims to provide seamless service provision from UNHCR, ARRA and partners, including some from the private sector. For that to happen, however, biometric data would need to be shared between these partners. In 2019 Ethiopia passed a law giving refugees the right to work and live outside of camps.[26] In order to enjoy these rights, it is critical that refugees have identification. In addition to giving individuals acceptable identification that then enables them to apply for drivers' licenses and bank accounts, digital IDs also make it possible for institutions to easily identify refugees as they access services and move around and outside of camps.

Relevant to the refugee contexts we explored in both Ethiopia and Bangladesh is UNHCR's firm belief that digital ID can empower refugees. The UNHCR Strategy on Digital Identity and Inclusion states, "A legal identity for every individual is of utmost importance. However, a digital identity that gives access to the internet, mobile phones and related services is equally becoming important."[27]

Nigeria: National digital ID

In our research in Nigeria, we learned about the country's national ID system, which is intended to integrate multiple pre-existing systems tied to specific government agencies. We also learned about a pilot program for an ID card tied to financial systems, which was the result of a partnership between the Nigerian government and MasterCard.

At least 13 federal agencies offer digital identity services in Nigeria, and most are not interoperable, forcing Nigerians to carry multiple IDs at once.[28] Each agency collects the same biometric information, multiplying the government's efforts and costs, creating competition amongst agencies, hindering coordination and creating more bureaucracy for cardholders.

A new system aims to merge all of these discrete systems to create a single digital identity for each individual and an atmosphere in which government agencies can work together. In col-

Oke Idanre in Indanre, Nigeria
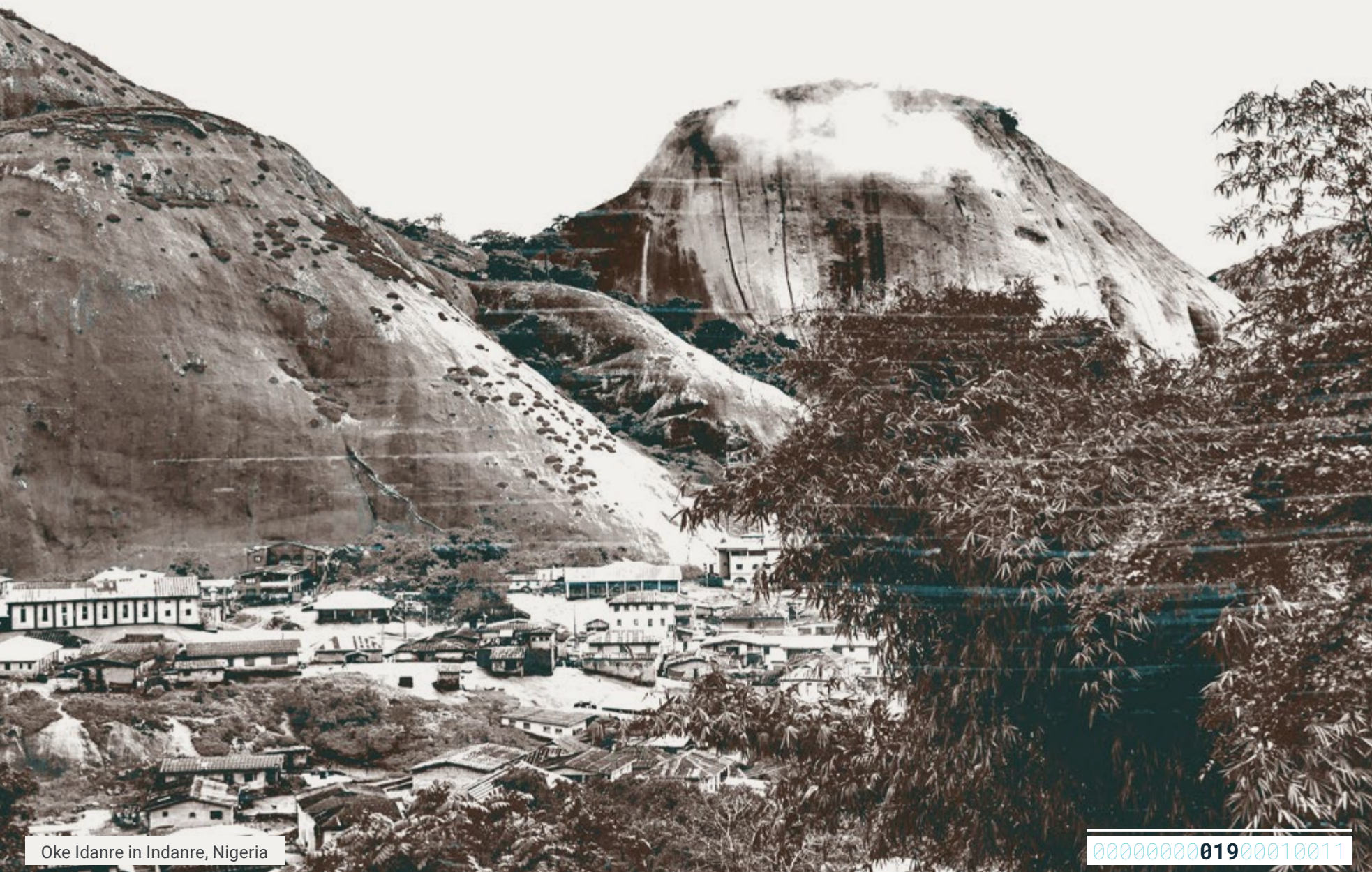
laboration with the World Bank,[29] Nigeria's National Identity Management Commission (NIMC) has developed an ecosystem approach to increase coverage of the national ID and make both public and private sectors enrolment partners. Financial inclusion is the main motivation for the country's new digital ID system; reports show that Nigeria has 60 million unbanked people.[30]

If the Commission meets its targets, this system will become the largest database in Africa.[31]

Not only will the new system be used across many government agencies, but also with a range of private sector institutions. A World Bank source told us they plan for:

> ... donor agencies, the UN, civil society to become enrolment partners with NIMC so that enrolment can happen at different points when you›re already trying to access a particular service or already trying to do another transaction. You›re not having to go enrol at NIMC and then also enrol for a bank account...and then also go enrol for your SIM card.

This will not be Nigerians' first experience with digital ID, however. In 2014, the Nigerian government introduced national biometric ID cards tied to the financial system and branded by MasterCard, marking the first time a major banking system directly endorsed a digital ID card,[32] though the company has since partnered with other countries. The scheme aimed to issue digital IDs to 13 million individuals but as of April 2018 had only issued 1.5 million IDs despite having taken 28.5 million registrations, leaving people unable to complete banking transactions and voting registration.[33]

The MasterCard-branded initiative also elicited concern from civil society, given its ties to a major US financial institution and the range of information (e.g., banking, social benefits, healthcare, travel) potentially shared with MasterCard. Activists and journalists criticised the pilot on socio-political grounds:

A Nigerian national identity card with a 'Mastercard' logo amounts to commercialization of our national insignia; its reminiscent of the logos of transatlantic slave trading companies, pasted on the bodies of Africans while they set forth for a cruel and dangerous journey across the oceans.[34]

Our field research in Nigeria focused on citizens' impressions of the forthcoming system developed by NIMC. Alongside its potential to become the largest digital ID system in Africa, Nigeria's is also the most interconnected system we examined. This makes it ripe for further research as more people register and use this ID for numerous transactions in their daily lives.

Zimbabwe: Biometric voter registration and national digital ID

Our research in Zimbabwe looked at two systems: a biometric voter ID card instituted in 2018, and a national ID system that is still in development.

Biometric Voter Registration

In 2018, Zimbabwe worked to phase out metal ID cards that had long served as the standard form of legal ID in the country. Authorities imposed a nationwide transition to a plastic biometric voter card, with multiple companies from outside of Zimbabwe managing different parts of the new biometric voter registration system.[35]

This transition took place approaching national elections in 2018, which marked Zimbabwe's first presidential election since the ousting of Robert Mugabe, who held the presidency for more than three decades. Civil society and opposition party representatives criticised the move to ban metal IDs, and the accompanying three-month registration exercise, fearing disenfranchisement and election rigging.[36] Additional problems ranged from the ruling party convincing people that the system could detect which way they would vote[37] to the hacking

Aerial view of a main street in Harare, Zimbabwe

of the Zimbabwe Election Commission's database, which led to the leaking of voters' personal and biometric data on the internet.[38]

National ID

Later that same year, the government announced plans for a national digital ID system. This system is intended to focus on financial systems and transportation security in partnership with the Chinese company CloudWalk Technology,[39] integrating artificial intelligence technologies into the digital ID system as part of China's Belt and Road initiative.[40] The agreement would give CloudWalk Technology access to a database of Zimbabwean faces to use as training data and improve the accuracy of their facial recognition technology, particularly on darker skin.[41] Digital rights and privacy advocates criticised this scheme as an avenue for both China and Zimbabwe to mine citizen data and refine surveillance practices. As Lynsey Chutel wrote for Quartz Africa, "It could very well be the latest example of Africa handing over natural resources to China for skewed compensation".[42]

The national digital ID system is part of Zimbabwe's national security agenda, and one focus group participant described the plan as part of "the militarisation of this country". Late former President Robert Mugabe's 37-year rule was marked by a wide range of rights violations, and the military that ousted him in 2017 retains significant power in policy making.[43] Already surveillance cameras have been installed in Harare, the capital, and concerns about privacy violations in relation to these cameras have been raised by civil society group MISA Zimbabwe.[44]

At the time of writing (November 2019), there was no indication of what stage the pending digital ID system is in. Due to the lack of transparency around this system, our research focused on people's experiences with the transition to the biometric voter card and their expectations for the new national ID, including its potential relationship to surveillance technologies.
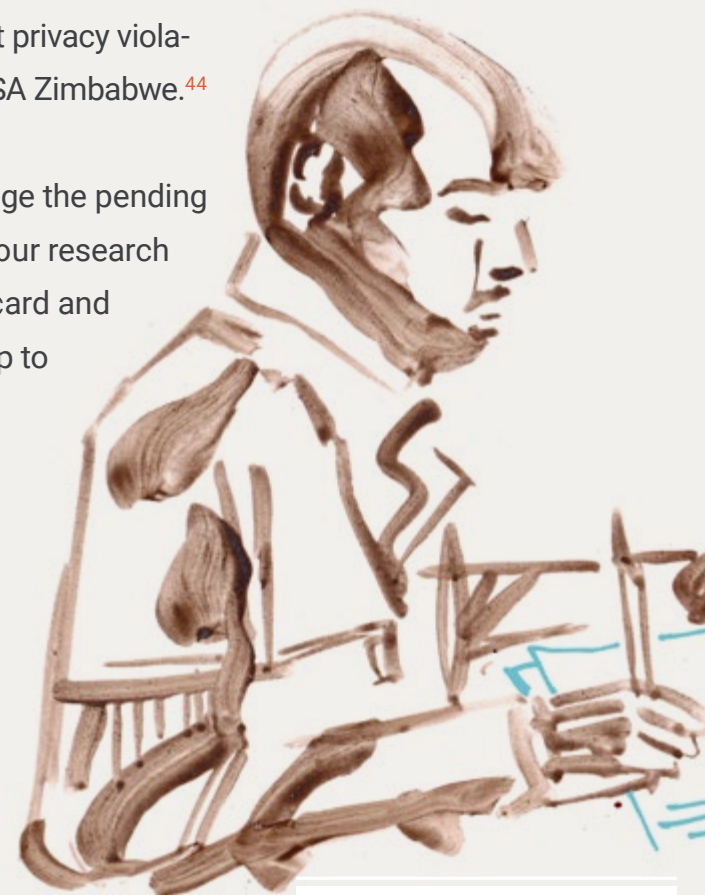
Thailand: National digital ID, 'pink card' for migrants and ID for people over 60 years of age

Thailand has a fragmented identity system, with multiple ID schemes for different populations administered by five different government departments at various levels of digitisation. Our research focused on what is known about the pending national digital ID system as well as the experiences of marginalised groups with current specialised ID systems, such as people eligible for a national ID reserved for those over 60 years old and migrant workers (primarily from Laos, Cambodia and Myanmar) who are given an ID known as the 'pink card'.

National ID

At the national level, Thailand is attempting to improve upon a failed effort at building a national digital ID system in 2004.[45] In September 2018 the government approved a draft bill to set regulations for authentication and require the formation of a 12-member committee to oversee the platform.[46] Delays have slowed the timeline significantly, and there is no indication of when the new system will be implemented.

The national ID card will be geared primarily towards promoting financial inclusion, to the benefit of government and financial sectors, but might also be linked to education and healthcare.

Digital rights advocates have expressed concerns that the new digital ID system will be no more useful than the previous system, will fall prey to software failures and privacy violations, and will be weakened by lack of faith in government systems.[47] Some also take issue with the cultural underpinnings of such systems: some Buddhists spoke out against digital ID in the past, saying these systems are incompatible with Buddhist dogma.[48]

Card for senior citizens

The card for people over 60 years of age has two benefits: financial support based on age and access to healthcare. People using the ID must remember a password, which focus group participants told us creates a barrier for those with memory issues such as dementia.

Migrant 'pink cards'

The Thai government introduced pink cards in 2014, with the intention of giving undocumented migrants a temporary ID that would allow them time to apply for passports and work permits, but the pink card remains in place.[49] Initially, more than 660,000 migrants from Myanmar and their families registered. Undocumented workers are required to register for the pink card through employers.

We were not able to ascertain whether or not the pink card is tied to biometric data for every individual, but we did learn that a wealth of information is collected from applicants and some migrants are made to submit DNA. As one government informant shared:

> Every year the Thai government has a quota (for security reasons) to take DNA samples from migrant workers. For those migrants who are randomly selected, they have to pay 25,000 BHT[50] to have a DNA sample taken at the public hospital.

The security reasons mentioned were not elaborated upon, however.

Silhouette of workers crossing the border for work in Mae Sot, Thailand
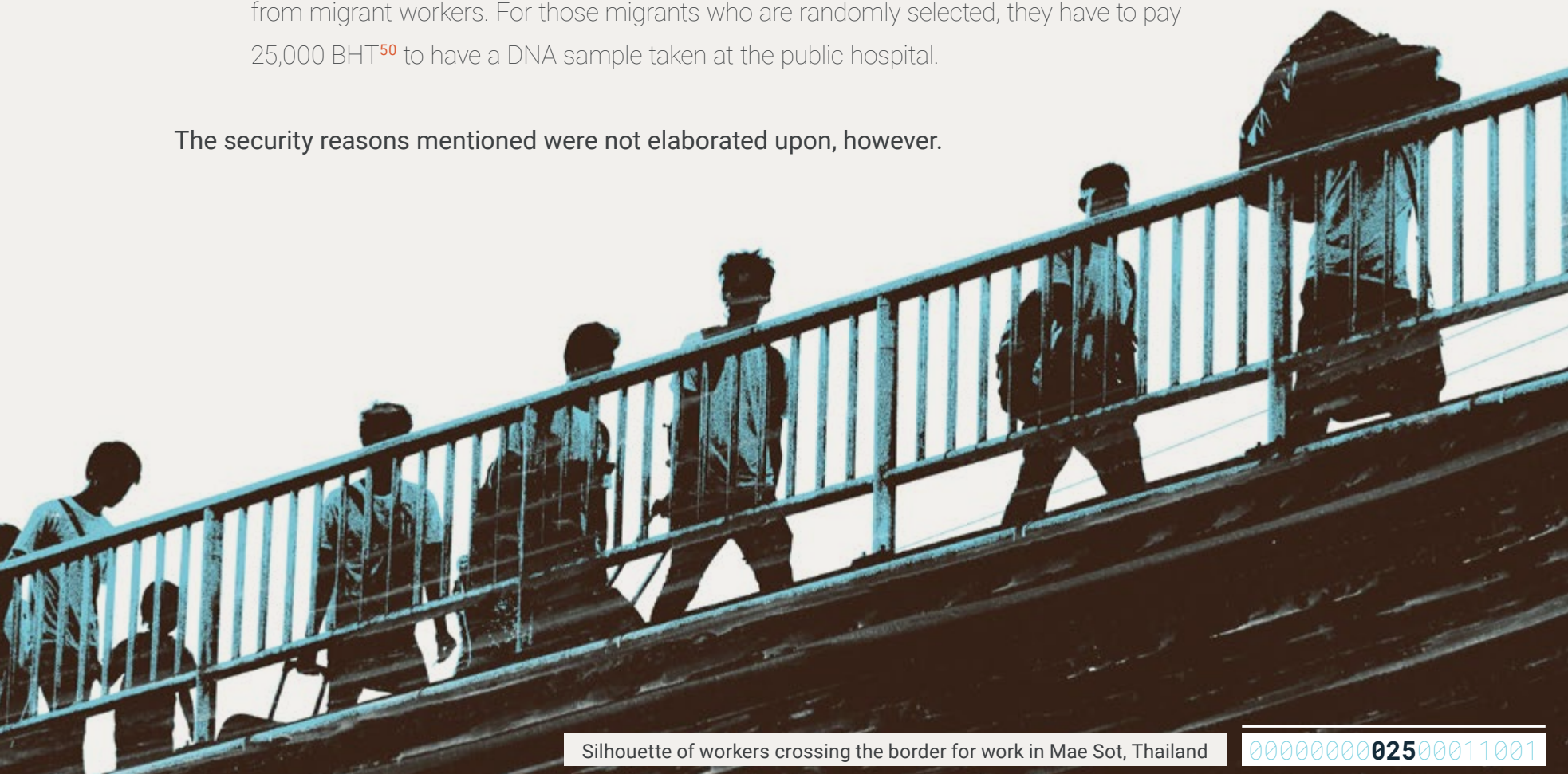
Key tensions

Through our work, we identified a number of key tensions. There are — or can be — real benefits to digital ID. Many of the problems these systems aim to solve are pressing, and the marginalised communities described in this report often face these challenges more frequently, and with deeper impact, than dominant communities.

We saw how powerful the benefits can be. We spoke to refugees in Bangladesh who were pleased to have received identification for the first time in their lives. UNHCR's plan enables forcibly displaced people in Ethiopia to leave refugee camps and settle in other parts of the country, accessing education and employment that promote self-sustainability, and most of the refugees we spoke to were happy about the opportunities they might find. Some focus group participants in Nigeria looked forward to having only one ID with many functions, and one study shows that Zimbabweans are "broadly satisfied"[51] with biometric voter registration despite its many shortcomings in the 2018 election. In Thailand, civil society organisations described how ID systems help the people they serve even though there are also harms. These benefits come at a cost, however. Key tensions that surfaced include:

1   **Digital ID can be a way to empower marginalised people while also increasing surveillance of, and subsequent rights abuses against, those same populations.**

2   **Digital ID can increase benefits for some populations while causing harm to others, further excluding them from social and other services.**

3   **Data sharing, centralised databases and merging IDs can create convenience but decrease data privacy, which can lead to the use of sensitive information (e.g., health conditions, financial difficulties) to restrict rights and opportunities.**

Of course, the motivation behind instituting digital ID systems is not homogenous. The institutions implementing the selected digital ID systems[52] aim to do one or more of the following:

- Ensure that people have acceptable identification that can enable access to everything from SIM cards to educational opportunities
- Provide a range of necessary and life-saving services (from voting and financial assistance for residents to food rations and international protection for refugees) more quickly and effectively
- Give people excluded from financial institutions due to a wide range of barriers access to bank accounts and financing
- Connect services, enabling easier transactions amongst a variety of government, NGO and private sector actors
- Improve public safety and decrease fraud
- Merge discrete systems, which will decrease the number of IDs people must carry and remember how to use as well as improve government efficiency by cutting out systems doing duplicated work

As presented in the research findings, however, these systems do not always achieve stated aims, especially not for all of the populations they serve. Elderly people in Thailand struggled to reap the card's benefits due to digital literacy barriers. Disabled people in multiple locations were unable to obtain cards due to physical and geographic barriers to registration. In all of the active systems examined we interviewed people who were unable to register or to use their IDs effectively.

There are also aims that benefit the institution developing the digital ID system. Zimbabwe's surveillance plans likely benefit the authoritarian state far more than any impact they will have on individual safety. Our research shows Thailand possibly using digital ID to monitor Indigenous people and human rights defenders and Bangladesh likely sending refugee data

to Myanmar.[53] Moreover, even if implementing institutions do accomplish objectives such as merging multiple ID systems, that success comes along with the problem of extensive data sharing, making it hard to follow who has access to what data on an institutional – let alone individual – level.

Behind the scenes of any digital ID system is a wealth of personal data – sometimes biometric, sometimes not. The more this data is shared, the more likely it is to be misused or hacked. People whose data is leaked can face life-altering consequences, including discrimination, public humiliation, financial costs, missed employment opportunities and termination, stalking and intimate partner violence, detainment, imprisonment and state violence.

Because digital ID data is tied to identities, it represents people – it is people, and that is sometimes easy to forget. Amid the digital ID cards, papers, or entries in a database, each data point represents some aspect of a person. The data that is gathered is intensely personal – names, dates of birth, addresses, health conditions, employment details, and in the case of biometric systems, that data becomes even more sensitive. If fingerprint images are leaked and misused by bad actors, what recourse do victims have? People cannot simply alter their fingerprints the way they change leaked passwords. The sensitive nature of the data collected through digital ID systems means that the way data is managed can have a huge impact on people's lives.

With all of these tensions, it is important to remember that institutions are, by and large, pushing societies towards a place where digital ID is a prerequisite for accessing vital services. This does not have to be the case, but if institutions decide that digital ID must go forward, they should consider how many systems compromise people's rights unnecessarily. Often, institutions prioritise their needs and priorities over individual or community rights, and, as our research shows, they privilege certain rights over others. People's right to food or shelter may be prioritised over the right to privacy,[54] for example. Given the risks associated

with data, numerous rights can end up being restricted or violated regardless of the intention of the operating institution. Using digital ID for national security can lead, intentionally or unintentionally, to violations of freedom of opinion and expression, freedom of assembly and association, and freedom of movement. Implementing digital ID in conjunction with surveillance cameras for public safety can actually violate the right to freedom from violence by enabling state violence against sex workers, religious and ethnic minorities and people with mental health issues.

Overall, there are tensions between public and private objectives but also between benefits and risks. The latter is complicated by the fact that the biggest risks lie with the people who have the fewest resources and the least political and social capital and that decision makers hold the most power and resources. Consequently, the latter group has a different perspective from those who are most affected by their decisions. The findings below prioritise the voices of people who are often ignored, allowing us to see more clearly what the risks entail.

Cross-cutting themes

The following themes were significant across all five sites, indicating common problems amongst digital ID systems:
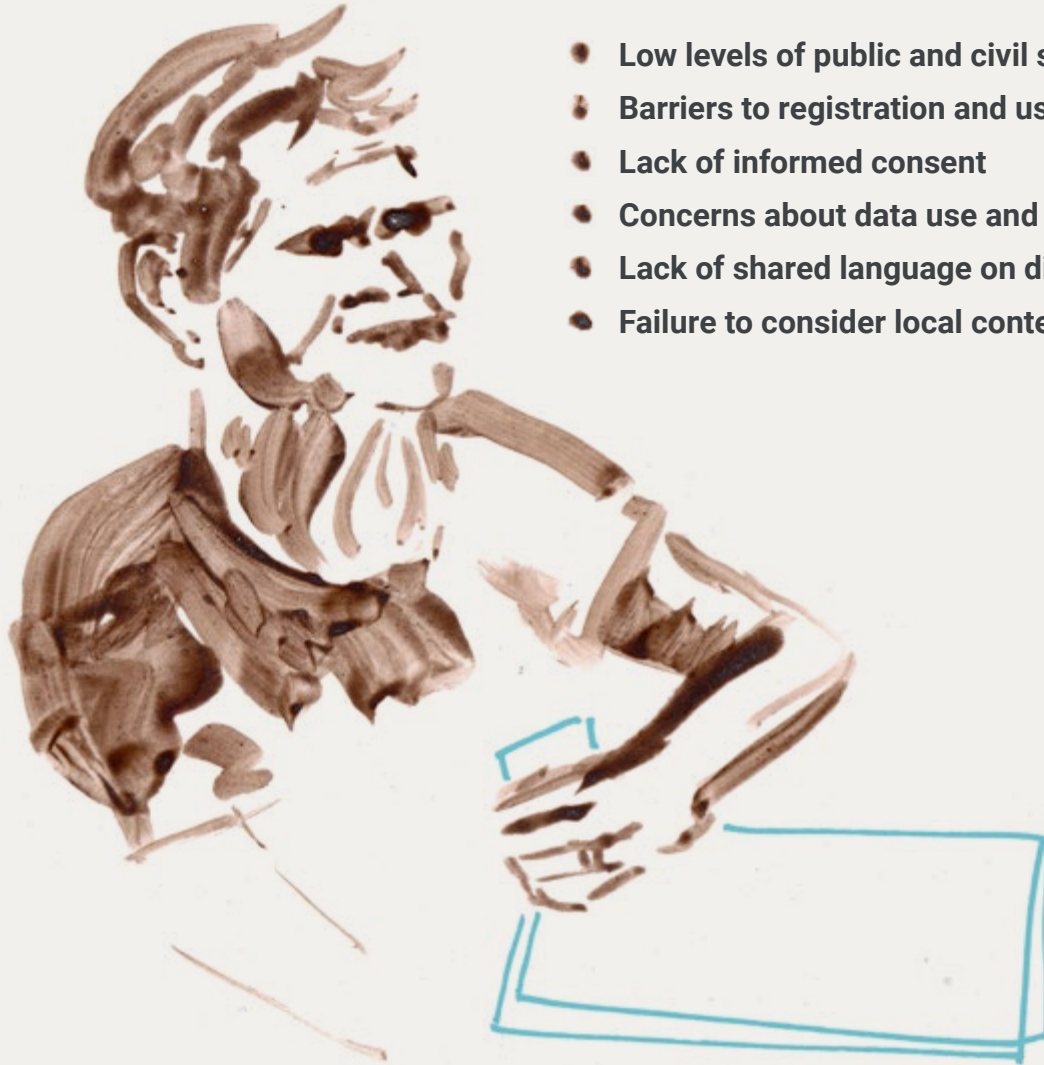
- **Low levels of public and civil society involvement**
- **Barriers to registration and use**
- **Lack of informed consent**
- **Concerns about data use and protection**
- **Lack of shared language on digital ID**
- **Failure to consider local context**

All of these issues can be major limiting factors in a community's support for digital ID and for their ability to fully enjoy its benefits. For a more detailed analysis of each of the selected systems, see the individual case studies, which cover themes beyond those included here. All quotations from key informant interviews and focus group discussions come from the field research phase in February-May 2019.

Low levels of public and civil society involvement

In all of the digital ID systems we examined, the aim was often to foundationally change the way people interacted with an institution or accessed services – often, to make interaction smoother and more convenient for individuals, while giving institutions a better overview of the people they sought to serve. These kinds of systems have the potential to affect a myriad of human rights beyond just privacy – from access to basic services like food and shelter to rights to dignity, freedom of movement and freedom of association.

Essentially, digital ID systems sit at the intersection of multiple rights, and the work of ensuring that one right is not sacrificed in pursuit of another requires meaningful and substantial input from people living in a variety of contexts. Across the systems we studied, however, there is a distinct lack of public awareness around the purposes and uses of digital ID systems, a lack of public consultation to inform the design and implementation of systems and a lack of civil society engagement to advocate for vulnerable communities. In our research, communities for which digital ID systems could be powerful for strengthening rights noted that they felt a distinct lack of ownership over these systems due to a lack of consultation.

People we spoke to across the five sites expressed concern over what purposes these systems serve. Beyond the rights violations involved in subjecting people to a system without their consent (see the section below on "lack of informed consent"), a failure to communicate basic information negatively affects the likelihood of success for any digital ID system. Infor-

mation gaps tend to lead to rumours, which can cause people to have false expectations. For example, in Bangladesh, Rohingya refugees feared that accepting smart cards meant automatic repatriation. This false impression meant that people did not register as requested, and when they were later 'obliged' to register for the ID, they worried about what they might have agreed to. Notably, many of the refugees we spoke to could not read at all, while others could not read English or Bengali, and thus had no way of knowing what was documented on their cards. In other locations, we found similar patterns of people not knowing what to expect, feeling hesitant, concerned or worried about the consequences, and trying to avoid digital IDs.

Additionally, a lack of trust between the implementers of a system and the people affected creates an environment where misinformation can easily spread. This is, of course, not unique to digital ID systems, but given that biometric digital ID systems often have unfamiliar processes (such as iris scanning), uncertainties about what these machines do in the absence of proactive information disclosure are unsurprisingly common.

Civil society groups that advocate with and for marginalised communities had similarly low levels of knowledge about digital ID. One exception was in Thailand, where an organisation we interviewed makes effective use of social media to provide information to migrant workers about the pink card, and has 200,000 migrant labourers accessing their services. This service evolved because much of the information on the pink card is only available in Thai and English, languages many migrant workers do not speak or read.

In fact, civil society engagement is a good way of building public awareness – that is, using civil society as an 'intermediary' layer, where implementing institutions consult with civil society, which then mobilises their existing connections and communities to gather feedback from diverse populations. There were a few examples of this activity – notably in Bangladesh, where local civil society and Rohingya activists in the diaspora have supported refugee rights and been active on the issue of digital ID.[55] In other countries, the most visible or active

groups on these issues come from a digital rights perspective, such as Paradigm Initiative in Nigeria and MISA Zimbabwe. Without a broader range of civil society engagement, however, advocacy is fairly limited to digital rights groups and perspectives.

Civil society across the five sites works under significant pressure with limited resources. Through our research, it also became clear that one of the biggest barriers to civil society engagement outside of the digital rights space was a lack of understanding of how digital ID affects the core issues they address, such as women's rights and disability rights. In some cases, too, the political environment makes it risky for groups to advocate on certain issues, Until recently, there were severe restrictions on civil society in Ethiopia,[56] for example.

Broadly speaking, there is a widespread trend of prioritising speed and more visible solutions (such as quantifiable issuing of ID cards) over approaches that might take more time and remain less quantifiable (such as public engagement or trust-building).This tension is particularly visible in the Rohingya case, where the Bangladeshi government was forced to respond to a massive influx of refugees from Myanmar with little preparation, significant uncertainty over how long the crisis would last and limited funds. We recognise that carrying out detailed and widespread public engagement takes time and resources, both of which are often in short reserve, especially in the humanitarian sector.

In cases where public consultation was carried out, institutions used shortcuts that prioritised some groups over others. In Bangladesh, for instance, a woman focus group participant told us that there had been discussions with men and boys about the system, but not women and girls. In Zimbabwe, knowledge of the system varied amongst focus groups. Some were aware, while others had so little information that they speculated that the system was kept secret "under the guise of national security".
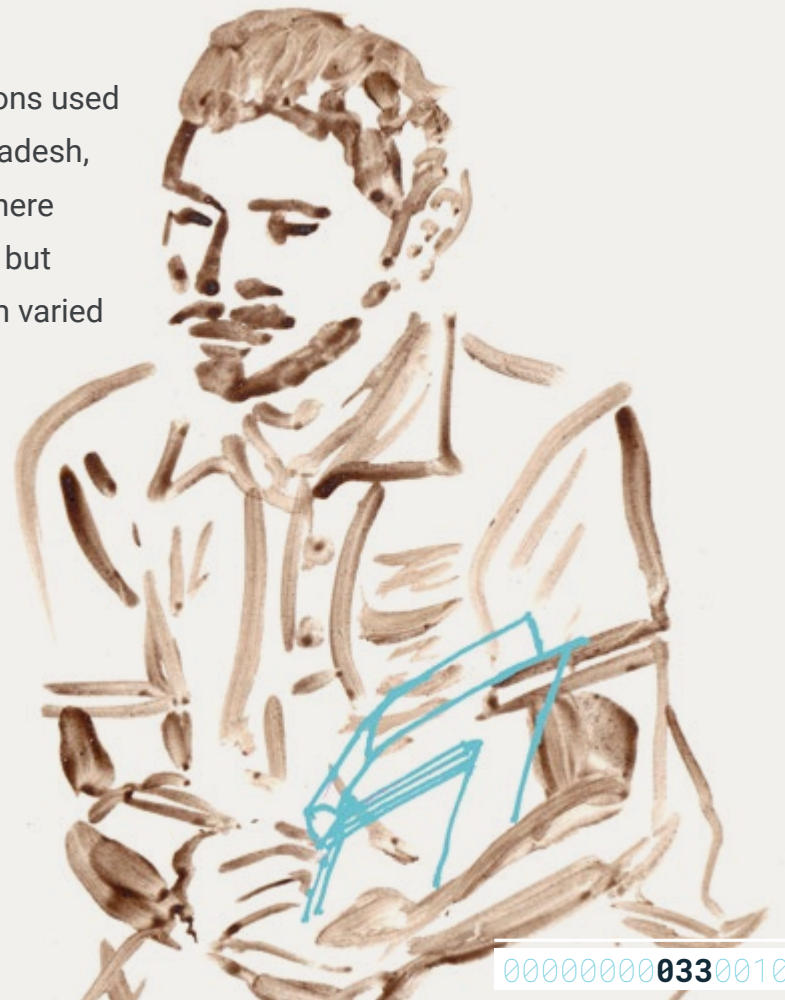
Most participants were not even aware of the differences between the metal and plastic IDs, including the fact that the plastic IDs contained biometric data and were machine readable.

Despite the lack of actual public engagement, many of the implementing institutions do acknowledge in their policies the importance of such engagement in rolling out successful systems. In some cases, this was a voluntary action: UNHCR has guidance on engaging with communities about the registration process[57] and committed to including refugees in consultations on digital ID systems from their endorsement of the 10 Principles on ID for Sustainable Development.[58] In Nigeria, the World Bank's digital ID development and implementation plan with the Nigerian government describes the importance of public engagement, including a stakeholder engagement plan with special attention to state governments, "regular communication with the general population" and "formal consultations with vulnerable groups".[59]

Barriers to registration and use

Across the board, we found a wide range of registration barriers, which are particularly concerning when IDs are necessary to access essential services. In particular, groups whose rights are already regularly violated – such as disabled people, transgender people and elderly people – are at risk of being further excluded by the registration processes used across different systems. This is particularly concerning given that the objective behind widespread implementation of digital ID systems is precisely to support and strengthen the rights of often-excluded groups whether through legal identity or financial inclusion. Registration can set the tone for how people's rights will be treated through this system, and their experiences in registration set their expectations, too: Will their needs be met, or will they struggle to participate?

Generally speaking, the way in which registration processes are designed does not seem to take into account the realities of the people expected to register. If registration locations are far from people's homes, especially those who live in rural locations, they have to walk long

distances to reach them. This is problematic for multiple reasons. Firstly, taking significant time away from regular activities might mean losing income or worse, losing a job. Secondly, travelling long distances is not possible for many disabled, elderly and pregnant people, leaving them unable to register without great difficulty. Finally, travelling longer distances alone may contravene cultural norms in some regions.

In Bangladesh, for example, some pregnant and disabled individuals were registered in their homes, but others had to walk all day to reach the registration centre. UNHCR disputes this claim, noting that registration centres are spread throughout the camps and that the longest walk would take approximately one hour. In Nigeria, many of the registration locations were not accessible to disabled people, but, notably, interviewees spoke of an alternative process for wealthier people who could pay registration officers to come to their houses and offices. Ultimately, those for whom ID cards could be most helpful in affirming their rights and accessing needed benefits are forced to stand in registration centre queues for up to days at a time, whereas people with more resources are able to obtain ID cards more quickly and without much trouble.

The prerequisites for registration can also serve to exclude, rather than include, certain populations. In Zimbabwe, people are required to have existing identification documents in order to register for a digital ID, but many do not, often due to difficulty with initial 'verification' of their identity resulting from errors on birth certificates or lack of information such as the name of a local chief. This seems counter-productive given that the original motivation of many of these systems is in response to Sustainable Development Target 16.9 – that is, to provide legal identity for all. In Thailand, the registration process for the migrant's pink card takes place through employers. In reality, migrant workers are operating under precarious employment conditions, and so they change jobs often. Connecting registration to employers, then, forces migrant workers to go through the registration process frequently, facing the same hurdles each time.

Other prerequisites of the Thai migrant workers system also ignore their realities, such as having application forms and information online only and not available in native languages of these populations. This forces them to rely upon exploitative brokers that offer short-cuts for a fee. These complicated and exclusionary processes do not bode well for Thailand's new national digital ID plans. As a basic first step for migrant IDs, making registration documents available in the major languages of primary migrant worker demographics would go a long way towards increasing system accessibility. The Thai government could learn some valuable lessons from the identity experiences of migrants and apply them to the pending national ID system.

If the registration process itself doesn't take cultural or social norms and realities into account, it can also serve as an extra barrier for people. This is another area in which adaptation to context is crucial in order for target populations to feel comfortable and able to participate fully with their dignity respected. In Bangladesh, women complained of being forced to free their ears and foreheads from their headscarves, remove jewelry and avoid wearing makeup. In some cases, registration staff removed or adjusted women's headscarves.[60] These women described feeling "disrespected", "upset", "uneasy", "humiliated" and "stressed" – far from the values of dignity that the humanitarian sector seeks to uphold. Similarly, in Nigeria women must choose between waiting in line with men, which, for some, goes against cultural norms and religious values, and not registering.

Existing prejudices can also be observed in the way that registration processes are carried out. Without explicit instructions to people implementing registration — and therefore in
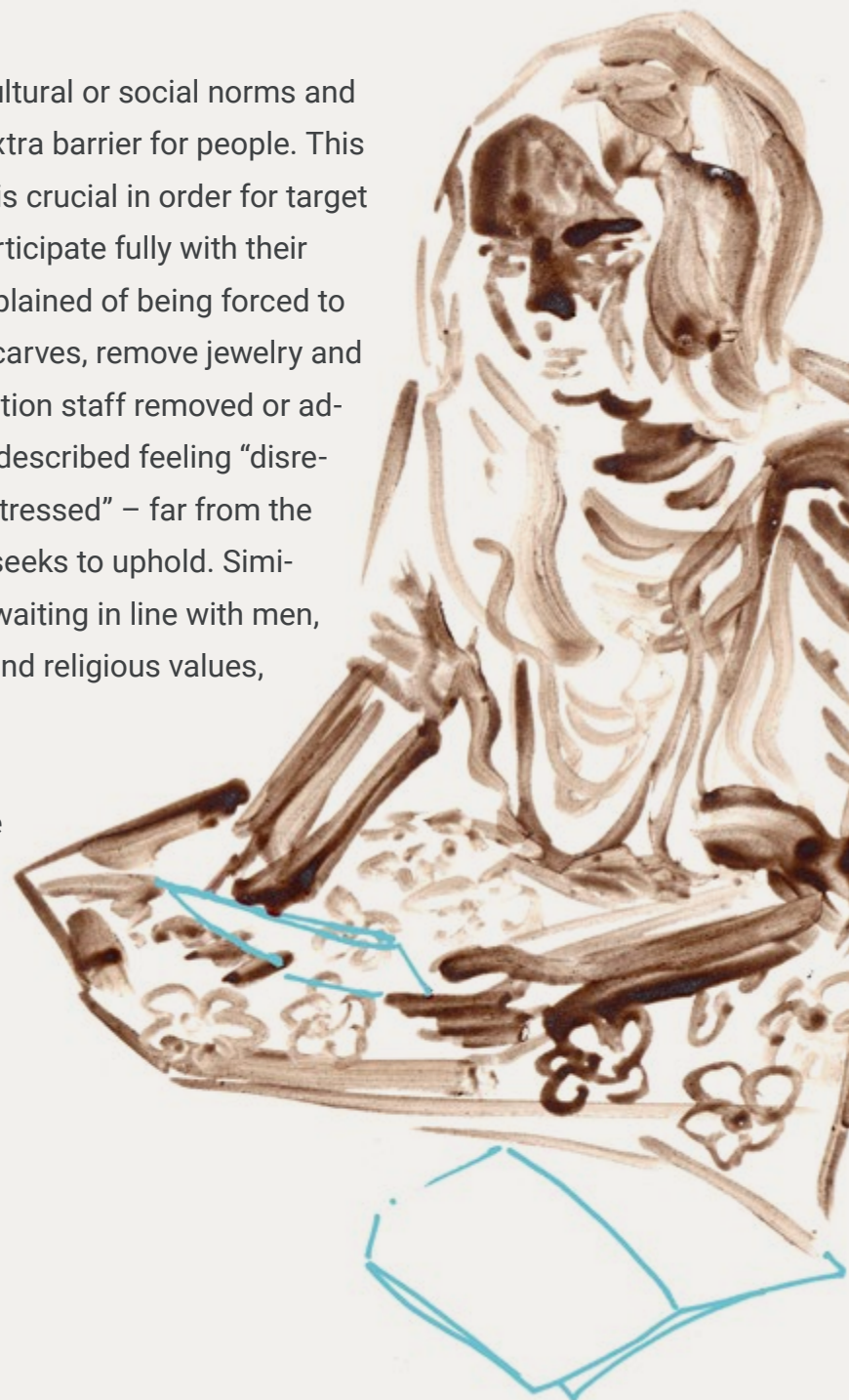
positions of power over people registering — to address these prejudices, digital ID systems will only further entrench these lines of exclusion. For example, transgender people in Zimbabwe face embarrassment and shaming by authorities who do not recognise gender as a social construct, and instead openly question people's gender and appearance according to their understanding of what different genders 'should' look like. In one case, a gender and sexual rights group described how one of their members had been harassed over their gender when they presented a passport that said they were female. Authorities insisted they looked male.

Finally, for people who can complete registration processes, it is reasonable to assume that mistakes will be made at times, particularly in humanitarian systems, where people registering are already in difficult situations and resources are low. However, across the systems we examined, the opportunities for data correction or redress were complicated, costly and sometimes fruitless. In Nigeria, for example, people must pay at least NGN 500[61] to make changes,[62] and one person told us they were charged NGN 1500 to fix their birth date.

We observed serious consequences of a few cases errors in Ethiopia. A refugee explained that her inability to prove her divorce, which took place in Eritrea, meant that she and the child she had after the divorce had been unable to complete the registration process. Another described arriving in Ethiopia sick, exhausted and filled with fear. Due to feeling disoriented at enrolment along with an inability to read, this person was unable to recognise that their birthplace was recorded incorrectly, a problem that remains unsolved and is a barrier to completing registration for a digital ID, though UNHCR says "evidence for a particular data-field is not a barrier to registration". UNHCR's guidance already addresses situations like these,[63] so it is possible that these cases are anomalies. Building in approaches to these non-standard cases would ensure that the most vulnerable can complete registration and access the benefits of an ID.

Similarly, in Thailand, migrants who encounter problems struggle to get support from officials, with one interviewee reporting:

> If we don't understand new rules, we used to call the hotline of Ministry of Labour, but no one picks up the phone or our calls have been transferred to several officials without any answer or any help. Sometimes, we face ignorance of officials and no care of officials who pick up the phone for inquiry.

Sometimes problems that start at registration create limitations for ID usage even when there are no data errors. One example can be seen in Nigeria, where many registration locations are not accessible to disabled people and there is confusion around recognition of disability. Registration forms ask people if they have disabilities but do not enable them to specify the type. The card itself does not include any information on disability, which caused disabled people we interviewed to be concerned about misunderstandings. A deaf person, for example, expressed concern that the card did not inform people of this disability, making the card less useful for that person. It is not clear if people scanning cards will then see information about a person's disabilities or for what purpose this information is collected in the first place.

Similarly, elderly people in Thailand face barriers to using their IDs. Since one of the functions of the ID card for this population is to receive welfare benefits, they must use the card to withdraw money from bank machines, but many focus group participants said they strug-

Voters at presidential election in Abuja, Nigeria

gle to use these machines and must rely on help. Some are able to get help from people they trust, while others complained of being forced to rely on strangers, which often leads to theft. By neglecting to assess whether or not a digital-first system would meet the needs of people who may have less digital literacy than other populations, the institutions imposing these systems leave older people struggling and facing additional threats.

Lack of informed consent

Within systems or processes that collect data from individuals, such as digital ID, it is generally accepted that informed consent should be obtained at the beginning of registration. However, in every system we explored, there were serious problems with informed consent. Informed consent is traditionally used as a way of protecting people from unethical practices carried out by institutions or people in positions of power.

UNHCR's internal Data Protection Guidance[64] indicates that they may only process data based on a "legitimate basis" (a term taken from language in the European Union's General Data Protection Regulation)[65] and stipulates that UNHCR are generally required to be "transparent, meaning clear and open with POCs [Persons of Concern] as data subjects about how their information will be used". But the guidance also states that:

> Consent is the most frequently used and often the preferred legal basis for personal data processing. However, given the vulnerability of most beneficiaries and the nature of humanitarian emergencies, many humanitarian organizations will not be in a position to rely on consent for most of their personal data processing.[66]

In our methodology, we considered this guidance alongside that which emerged from the Nuremberg Trials to protect human research subjects.[67] The key tenets[68] of informed consent are generally understood to be some combination of:

1 **Voluntariness:** A person gives their agreement free of coercion or pressure and without negative consequences for declining

2 **Disclosure:** The burden of sharing information about the process is on the powerful person/institution making the request

3 **Understanding:** The person fully understands what is happening

4 **Capacity**, sometimes called competence: The person is in a position to fully comprehend the information and process

5 **Assent/Consent:** The action whereby the person actually agrees to the request or process

In our field research, there were no systems where implementing institutions followed all five tenets. Often, none of the five tenets was present. Consent in these systems can be considered a proxy for how power asymmetries are addressed: building in checks and balances, non-punitive ways for people to make free choices without coercion, and, above all, avenues for them to fully participate while having their dignity and right to privacy respected.

We observed that people who were subjected to these systems often had very low expectations of how their rights should or would be respected through the system. In Nigeria, people we interviewed told us that turning up at a registration centre was synonymous with giving consent, making it unlikely that they would demand a more rights-based approach or that the government would voluntarily provide one.

Nowhere is this problem clearer than in the refugee use case, however. Bearing in mind that people we spoke to in Bangladesh had recently fled serious, targeted violence, they saw the Bangladeshi government as benefactors to whom they should be grateful and not ask ques-

tions. One refugee said, "The country that feeds us, we will have to follow their command," and others described themselves as "being under their [UNHCR/Bangladesh] rule now".

These comments highlight vital issues beyond consent, including expectations for the behaviour of institutions in positions of power, the responsibility of those institutions, and subsequently, the limitations of current accountability mechanisms. If people expect that institutions can treat them as those institutions like and the people should be grateful for whatever happens, then they are not in a position to directly hold those institutions accountable for their obligations under local law and international human rights doctrine. This demonstrates the need for advocacy organisations that work to inform refugees of their rights and support them in using available accountability mechanisms. Presently, however, there exist very few meaningful accountability mechanisms for humanitarian organisations working outside of their home jurisdictions and for states that have not signed treaties and conventions such as the 1951 United Nations Convention Related to the Status of Refugees.[69]

Alongside conflated expectations were misinterpretations of who is ultimately responsible for broader assistance provision. Rohingya refugees recognised the power of the Government of Bangladesh, rather than the power of UNHCR, in providing them with assistance.

Rohingya camps in Cox's Bazar, Bangladesh

Community leaders talked about feeling grateful to the Bangladeshi government for their assistance and fearful of UNHCR, whom they suspected of working against their welfare. They put their trust in the government and not in humanitarian agencies.

Within the humanitarian sector, the 'voluntariness' aspect of informed consent is difficult, if not impossible without alternatives to digital ID systems (which might require gathering less, or different, data), including facing no change in services or assistance as a result of refusing to provide consent and complete registration. Establishing a parallel process would, undoubtedly, require more resources than simply having one digital ID system at play but would give people some control and freedom to decide what happens to their data. This freedom becomes particularly critical when digital ID systems rely on fairly immutable data derived directly from refugee bodies. Ultimately, what happens with these systems may come down to a question of priorities. What is prioritised – people's dignity and agency, or system efficiency?

Increasingly, humanitarian organisations are discussing problems with informed consent. The International Committee of the Red Cross announced in October 2019 a new biometrics policy that recognises that consent cannot be "freely given" in humanitarian contexts but also goes beyond previous approaches to emphasise

One rare experience of demanding change around digital ID in refugee camps came about in Cox's Bazar. In November 2018, Rohingya refugees staged a three-day strike[70] against UNHCR's digital ID system because they wanted their ethnicity clearly labeled on the IDs (against UNHCR protocol) as a way to preserve their Myanmar citizenship and theoretically prevent further target violence upon repatriation. The success of this protest was two-fold: refugees received more information about the ID system and the purpose of the cards, and they were satisfied that their proof of registration form documented their ethnicity. The people's capacity to protest may have been due to their partly mistaken assumption that the host country provided for them while UNHCR and NGOs, in the words of an imam we interviewed, "don't think about our well-being".

choice.[71] The ICRC states, "If people do not want to provide their biometric or other personal data, or to see their information shared for humanitarian purposes with partners, the ICRC will respect their wishes."

In the camps we visited, refugees appear to have no choice but to provide biometric data to UNHCR and host governments if they want assistance. Multiple UNHCR informants reported that beneficiaries who refuse to share their data as part of the registration process will not receive aid. One informant reported:

> If they do not finish the BIMS[72], it is difficult to attain proof of registration, which is a document we give them at the end of the registration. He or she who does not hold the proof of registration will not receive assistance.

This was confirmed by UNHCR officials. UNHCR staff in Ethiopia described the procedure for handling refusals: individuals are sent to the litigation desk where they receive further information about the use of their biometric data and are warned that they risk losing assistance if they continue to refuse. None had ever witnessed a refusal. This is unsurprising given that refusing consent is tantamount to refusing assistance when people are already vulnerable and hungry. Refugees are aware of the consequences of refusal, with one man describing what UNHCR said to him as "you will have to take the card. Otherwise you won't get rations."

As demonstrated in the section above on awareness, proactive information disclosure was also lacking in the systems we examined. In both refugee cases, people were unsure about the purpose of the data being collected and were sometimes given false information.
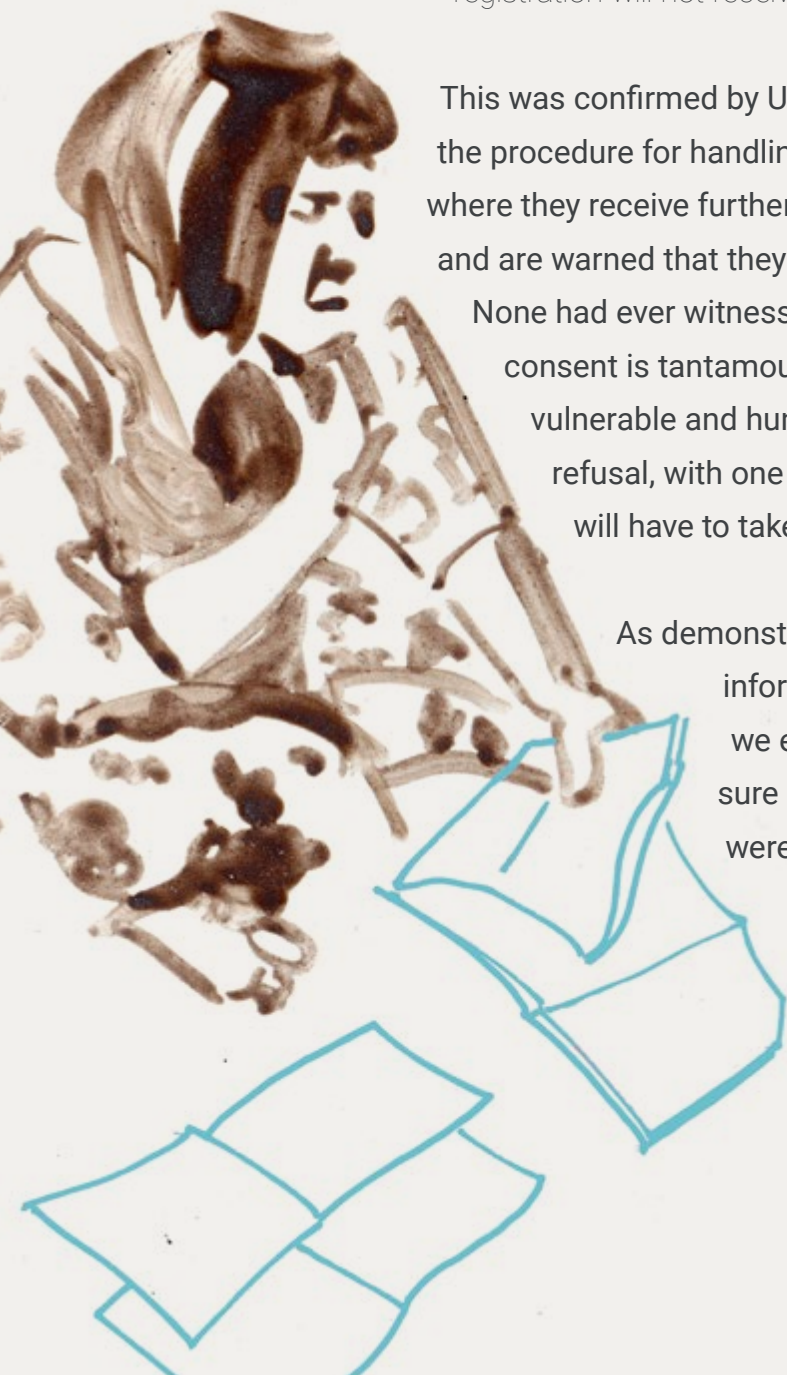
Notably, some refugees in Ethiopia thought the iris scans were checking for disease. A woman who was confused about the iris scan said, "They did something to our eyes using a large pipe. They did something, I could see another pair of eyes in there."

Even when people take it upon themselves to demand or ask for information, which shouldnot be required of them, details are not always provided. In Ethiopia, many interviewees expressed frustration that they were not given information and their questions were not answered. Our researcher also observed registration processes at Histas camp and noted that refugees were "told to look into the binocular that records their iris and provide their fingerprints without an explanation of what it does or why they are providing this information".

As stated previously, although it allows for exceptions, UNHCR policy is to obtain consent for registration,[73] as is the case with other refugee-serving institutions. While the behaviours we observed in Bangladesh and Ethiopia may not be every refugee's experience, these findings echo research results in other humanitarian contexts, including reports on refugee experiences in Europe by Dragana Kaurin[74] and Data & Society,[75] both of whom found that informed consent for refugees in European Union humanitarian aid systems[76] was rarely sought and rarely meaningful.

It seems that the reality around consent in the field often devi-

ates from best practice and from internal policies. These discrepancies raise questions about how far organisations go to make sure their guidelines are viable in local contexts and operationalised adequately. They also raise questions about how local humanitarian staff implementing registration are trained and monitored.

Underlying the key tenets of informed consent is another major issue: trust. If people lack trust that implementing institutions treat their data as promised, then the process loses much of its value. In other words, what good is information disclosure if people expect the information to be false? Discussions with Thai people in a Good ID workshop[77] held in Bangkok revealed that, by and large, the Thai population lacks trust in biometric systems. If people cannot trust a system and the people running it, informed consent becomes relatively meaningless.

One way to build trust is by adopting rights-affirming data protection legislation that enshrines peoples' rights to own and control their personal data, requires transparency by institutions that collect personal data, and provides consequences for violations. Many countries still do not have data protection laws that address the type of data gathered through digital ID systems. Zimbabwe's Access to Information and Protection of Privacy Act (2002), for example, does not include biometric data or cross-border data sharing, and the country's omnibus Cyber Crime, Security and Data Protection Bill, which could provide some necessary protections, is still up for debate[78] and has been criticised by digital rights advocates.[79] If the government does go forward with an international commercial partner, in China or elsewhere, that company could collect a wealth of data on Zimbabwean citizens, who are powerless to object – and who, ultimately, might not even be actively told about this development.

Concerns about data use and protection

Despite the major impact collection of sensitive data can have on people's lives, there is little transparency about data use and protection decisions across most of the systems we studied, leaving many people wondering who sees their data and how it is used.

To prevent data misuse, there should be strong and enforced data protection legislation in place before digital ID systems are set up, but this is rarely the case. In some cases, we found there to be a lack of relevant legislation; in others, legislation was not comprehensive enough or was combined with bills clamping down on other rights. For example, it is unclear whether or not data protection for Bangladeshi citizens issued under the Digital Security Act of 2018,[80] which also restricts freedom of expression,[81] would extend to refugees in the absence of a refugee protection framework.

In early 2019, Thailand passed the Personal Data Protection Act,[82] which is informed by the European Union's General Data Protection Regulation and an important step in the right direction, but, as with Bangladesh, it is not clear if this law and any follow-up legislation will apply to migrants.

UNHCR has data-sharing agreements with host countries that detail why and how data can be transferred, but we were told that "governments are often co-collecting with UNHCR, so where a government collects and holds data...UNHCR can only advise (and not control) how a government manages its data". Fortunately, in 2019 Ethiopia adopted a new refugee law[83] that addresses data privacy. Most importantly, the law bars the disclosure of refugee information to the authorities of countries of origin. At the same time, the country has no data protection law in place for citizens, though informants told us Ethiopia is considering a national digital ID system based on UNHCR's system.

Many issues around data protection arise from the beginning of a digital ID project. Often, in order to implement digital ID systems, institutions and governments form agreements with commercial partners that have the technical capacity to build and maintain systems, but contracts with these partners are rarely, if ever, made public. Nigeria's digital ID system will be used across several government agencies as well as some private sector companies, yet Nigeria lacks data protection laws. Without laws and transparency around data-sharing agreements, the people of Nigeria have no idea who might see their data.

These partnerships can also create long-term dependency on the contracted company, which may hold people's data and run the system itself. This is known as 'vendor lock-in', where institutions are forced into continuing to work with a certain vendor no matter the cost or condition because the alternative would be to lose access to an entire system (and the data held within – or, sometimes, even if the data can be exported, it cannot be re-used without access to that proprietary system). With proprietary systems, institutions and people may be reliant on these vendors to keep data secure without being able to independently assess and verify the efficacy of the software.

In Bangladesh, some Rohingya people are deeply concerned about their data being used for repatriation and shared with the Government of Myanmar: "What if they give our information to the Burmese government…and what if they make a connection between the smart cards and NVC [National Verification Cards] and hand us our NVC cards forcefully?" Thus far, there have been rumours and reports[84] of the Bangladeshi government handing over personal data of the Rohingya to the Myanmar government that targeted this population with violence in the first place.[85] On the other hand, several focus group participants could see benefits in sharing this information with Myanmar, imagining a smoother repatriation transition and having their citizenship recognised.

Another concern for many people we spoke to was the idea of personal data being shared across government agencies and with community institutions. Almost everyone we spoke to in Zimbabwe has a group in mind that they would rather keep their personal data away from. For example, activists did not want their data shared with political parties, churches and universities, while people living with HIV wanted their data kept out of the hands of the ruling party, police, certain NGOs and churches. Sex workers, transgender folks and farmers expressed concern about the police and military, forces that already made their lives difficult. Indeed, digital ID systems often gather data that, in the wrong hands, could be used to target and persecute people whose rights are already at risk. Those groups often (understandably) have low levels of trust in institutions, a problem compounded by lack of rights-affirming legislation.

Systems that aim to unite multiple databases and platforms – such as Thailand's talk of citizens using one card for everything, with "all their information in one data centre to which every government agency has access" as described by the Director of the Bureau of Registration Administration – by necessity have a lot of data sharing built into them. This can make things more convenient for people who no longer have to obtain and use separate cards for different purposes, but it can also have severe consequences for people who might be most in need of bureaucratic support. A women's rights group in Thailand raised the issue of trafficking survivors being "blacklisted" by financial institutions, unable to get loans or extend their passports, because of data that showed a history of working in the sex trade.

Additionally, an Indigenous rights group[86] we interviewed described Indigenous people and human rights defenders being surveilled at borders, although these claims have not been confirmed:

> With consideration of public benefit and national security and no respect to individual
> rights, government officials use digital information to spot most Indigenous people living

along borders, especially environmental and human rights defenders and track their political movement and border crossing.

Ultimately, if people cannot trust authorities to use their data as stated and to protect their data, they will be less likely to reap the benefits of digital ID and already marginalised groups will be further excluded. Institutions developing digital ID systems should not move forward until robust legislation has been passed and implemented.

No shared understanding of digital ID

In relation to awareness, researchers found that some in-country languages have not (yet) developed agreed translations for key terms, such as 'digital ID' or 'biometric data'. On a micro level for this project, this meant that researchers spent significant time explaining and describing rather than building upon a shared understanding. On a macro level, the lack of agreed terms indicates a low level of in-country dialogue about these systems and/or a perceived lack of ownership of the systems.

A market in Huaikoan, Nan, Thailand, on the border with Laos

As well as the lack of literal translations, the systems themselves – the scope and reach of the systems – were also hard to define. Low levels of technical literacy around the concept of digital ID are in keeping with digital literacy challenges more broadly, but not understanding these technical systems can have wide-reaching impacts upon the ability of citizens to engage in their societies. This, again, speaks to the lack of transparency around the scope of many of these systems.

The UNHCR language of 'verification process'[87] in Rohingya refugee camps in Cox's Bazar, Bangladesh, is easily conflated with Myanmar's deeply problematic National Verification Cards. With little understanding of the benefits of this process and little knowledge of what is happening when biometric data is collected, even the resulting 'smart card' becomes a fairly empty term and the system's consequences become harder to understand. How is the card 'smart'? What information does it hold? Even in Ethiopian camps, where people generally understood that their information was captured and held digitally, many were unfamiliar with the intended use of digital identity.

The definition of what is and is not a 'digital ID' system was unclear across the research sites we considered. In some cases, digital ID systems were understood, by definition, to include biometric data, while in others, they were seen as general digital ID systems that may or may not collect biometric data. This is unsurprising given, as outlined above, a lack of public engagement and consultation, as well as confusing messaging about system purpose and scope.

These confusions were further compounded for people with lower levels of technical literacy, such as older people in Thailand or Rohingya refugees who had not interacted with complex digital systems before. Additionally, the fact that many systems were fragmented (as in Thailand, where people were interacting with multiple systems without necessarily knowing it) made it even harder to define or establish the scope of the various systems.

Failure to consider local context

Digital ID systems are sociotechnical systems; they sit within existing social, political and cultural contexts. As such, though a system might follow what is commonly understood to be 'global best practice' or simply be a replica of another country's approach, it is likely that some adaptations to the new context will be necessary. As more countries and institutions set up digital ID systems, there is a push for best practices or norms to be established.[88] Given how deeply rooted digital ID systems are in personal preferences and cultural worldviews, however, establishing global norms becomes difficult.

This complexity is most clearly seen in how Rohingya refugees have pushed for their ethnicity data to be explicitly stated on their IDs.

Repeatedly, ethnicity data has been used to divide populations and facilitate targeted violence – from the way data was collected on Jewish and Roma populations during the Nazi occupation of the Netherlands, leaving Dutch Jews with the highest death rate among all other occupied western European countries, to Rwanda, where ID cards identifying people by their 'ethnic group' served as an effective death sentence in 1994.[89] Because of these travesties, the best practice is not to document ethnicity without good reason, and if it must be documented, to keep it separate from other personally identifiable data.

It is understandable why UNHCR did not print ethnicity on the smart cards given to Rohingya refugees, but context for the demands of this refugee community is critical. In Myanmar, the ID cards issued to Rohingya Muslims labelled them as 'Bengalis,' denying their Myanmar citizenship. In Bangladesh, the cards they receive label them as being "from Myanmar", which Rohingya refugees argue similarly denies their Myanmar citizenship. For Rohingya refugees,

the most powerful role of an ID card would be to counter erasure of their ethnicity and citizenship, and for this reason, in November 2018, many staged a three-day strike[90] against UNHCR's digital ID system in part to demand documentation of their ethnicity on their smart cards. This would serve to assert their Myanmar citizenship and theoretically prevent further targeted violence upon repatriation, although there is no guarantee it would be accepted as such by Myanmar authorities.

Overall we saw relatively little adaptation of systems to specific contexts. Reasons behind this are multifaceted. As described above, there are few lines of communication between affected people and implementing institutions. Additionally, governments and organisations sometimes contract commercial sector partners that implement the same system across different contexts. While designing from scratch for each implementation would undoubtedly be a waste of resources, we observed a great need for more flexibility and adaptation to the realities of people in order to make systems as useful as possible.

Rohingya camps in Cox's Bazar, Bangladesh

Conclusions and Recommendations

This report outlined cross-cutting themes across five digital ID systems in Bangladesh, Ethiopia, Nigeria, Zimbabwe and Thailand. The research makes clear that digital ID systems are sociotechnical systems that exist within diverse contexts and sit at the intersection of many distinct human rights.

Through this project, we have observed that working on digital ID means working across typically siloed spaces and sectors. Digital ID effectively collapses those divisions due to the cross-cutting way it touches a multitude of areas, and while the digital rights sector has been quick to recognise that digital ID intersects with their areas of focus, other civil society actors have not. We have seen again and again that digital rights cannot sit as a separate issue to more 'traditional' human rights, such as the right to food, shelter, or water, if all are to be respected.

In order for civil society to adequately mobilise on issues of digital ID, we need a more holistic approach that acknowledges how our societies are building dependence upon formal identification documentation systems. Within those systems, access to digital ID could indeed bring great benefits to communities that have struggled to be seen and understood by states and institutions. Self-identification for transgender people can be hugely empowering. The ability for women to identify as heads of households and access benefits can affect generational changes. Refugees wanting to fight erasure of their ethnicity and migrant workers seeking to be acknowledged by states when they are mistreated by employers can do this through a rights-respecting digital ID. All are examples of the positive potential impacts of context-respecting digital ID systems.

At the same time, digital ID systems raise serious concerns around inclusion, privacy and individual agency. We see an increased push for centralised systems that reduce friction on the side of the implementing institution without adequate concern for the consequences of such widespread data sharing. Across the board, there is a real lack of transparency regarding decisions about systems. In particular, partnerships with the private sector mean that how data is shared, where it goes and who has access to it are increasingly unclear. For biometric data, this could have irreversible consequences.

As systems grow, more data is gathered and more institutions gain access to that data, we must advocate for stronger, enforced, rights-protecting legislation. In order to take advantage of digital ID systems, civil society must engage on these issues in a proactive, rather than reactive, way. We have seen great wins in Kenya,[91] India,[92] Tunisia[93] [94] and Jamaica,[95] where advocacy with lawmakers reduced the risks that digital ID systems created for people's rights or even stopped planned systems altogether. If implementing institutions truly seek to achieve public-facing aims of enabling participation in society for those without formal identification, then they should welcome civil society involvement.

For a rights-based approach to digital ID, we need a plurality of civil society advocating around digital ID. It is undeniable that digital ID systems are spreading, but how they spread, the decisions underpinning them, and their relation to a range of rights can be guided by local communities.

Based on this research project, we put together the following recommendations for people advocating for change around digital ID. As we did not focus on technical infrastructure of digital ID systems, these recommendations focus on social, cultural and legal aspects, and are intended as a non-exclusive set of recommendations.

We recommend that people advocate for institutions developing and implementing digital ID systems to:

1 Prioritise meaningful public and civil society involvement and engagement throughout the project.

    a. From creation and design through implementation, ensure that easily accessible information about the system is proactively shared in a way that reaches diverse members of society.

    b. Carry out ongoing public consultations rather than one-off opportunities, and ensure that people whose rights are often denied, such as disabled people, el-

derly people, low-income people, informal labourers, rural residents, ethnic and religious minorities, migrants, sex workers and LGBTQI groups, are included.

c. Build relationships with a range of civil society organisations that can provide feedback to strengthen the system.

d. Set up multi-step feedback processes to ensure that both negative and positive feedback will reach influential people and inform improvements and iterations of the system.

2 Establish and follow policies and legislation that protect the rights of people affected by a digital ID system.

a. Focus on rights-affirming legislation that prioritises the needs of the people over the interests of the implementing institution.

b. Design grievance-reporting mechanisms and processes to address problems in a timely manner.

c. Consider how power asymmetries will affect informed consent and develop policies reflecting these imbalances. If informed consent cannot be meaningful in this environment, explore ways to replace or further support consent processes in order to respect people's rights and dignity.

3 Recognise the importance of social, political and cultural context and design systems that meet these contexts in a respectful way.

    a. Ensure that information and all steps of the system are provided in relevant local languages, including those of significant migrant populations.

    b. Establish a community engagement plan to understand:

        I. The cultural perceptions that could affect system roll-out, especially if biometric data is included

        II. What a meaningful informed consent process could look like

    c. Ensure key processes throughout the system, including registration, renewal, grievance reporting and legal support are accessible.

4 Provide ongoing training for staff implementing or involved in digital ID systems.

    a. Ensure staff have access to regularly updated guidance on how to engage with people and what information to provide.

b. Ensure onboarding of new staff includes a focus on the context of a digital ID system and other key policies such as data protection.

c. Train staff to invite questions and answer them respectfully, and ensure supervisors conduct regular reviews of staff interaction with target populations.

d. Create internal space for staff to share major barriers they face in registering people, the grievances people express to them and ideas for solving these problems.

Notes

1   World Bank. (2018). Principles on identification for sustainable development: Toward the digital age. http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf

2   United Nations. (2015). Goal 16 | Sustainable Development Knowledge Platform. https://sustainabledevelopment.un.org/sdg16

3   See, for example, Privacy International's work at https://privacyinternational.org/topics/identity and Access Now's efforts at https://www.accessnow.org/cms/assets/uploads/2018/03/Digital-Identity-Paper-digital-version-Mar20.pdf

4   Gelb, A., & Clark, J. (2013, January). "Identification for Development: The Biometrics Revolution". Center for Global Development Working Paper 315. https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315

5   OHCHR. (2019). Sexual and gender-based violence in Myanmar and the gendered impact of its ethnic conflicts. Human Rights Council. https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/sexualviolence/A_HRC_CRP_4.pdf

6   UNHCR. (2019). Bangladesh Rohingya Emergency. https://www.unhcr.org/ph/campaigns/rohingya-emergency

7   UNHCR. (2018, July 6). Joint Bangladesh/UNHCR verification of Rohingya refugees gets underway. https://www.unhcr.org/en-us/news/briefing/2018/7/5b3f2794ae/joint-bangladeshunhcr-verification-rohingya-refugees-gets-underway.html

8   Ibid.

9   McPherson, P., Lewis, S., Aung, T. T., Siddiqui, Z., & Naing, S. (2018, December 18). Special Report: Myanmar's moves could mean the Rohingya never go home. Reuters. https://www.reuters.com/article/us-myanmar-rohingya-return-special-repor/special-report-myanmars-moves-could-mean-the-rohingya-never-go-home-idUSKBN1OH1AK

10   Milko, V. (2019, September 3). "Genocide card": Myanmar Rohingya verification scheme condemned. Al Jazeera. https://www.aljazeera.com/news/2019/09/genocide-card-myanmar-rohingya-verification-scheme-condemned-190903012922259.html

11   Fortify Rights. (2019). Tools of Genocide—National Verification Cards and the Denial of Citizenship of Rohingya Muslims in Myanmar. https://www.fortifyrights.org/downloads/Tools%20of%20Genocide%20-%20Fortify%20Rights%20-%20September-03-2019-EN.pdf

12   Ibid.

13   UNHCR. (2018, July 6). Joint Bangladesh/UNHCR verification of Rohingya refugees gets underway.

https://www.unhcr.org/en-us/news/briefing/2018/7/5b3f2794ae/joint-bangladeshunhcr-verification-rohingya-refugees-gets-underway.html

14   Ellis-Petersen, H., & Rahman, S. A. (2019, August 22). Rohingya refugees turn down second Myanmar repatriation effort. The Guardian. https://www.theguardian.com/world/2019/aug/22/rohingya-refugees-turn-down-second-myanmar-repatriation-effort

15   Ahmed, K. (2018, November 27). In Bangladesh, a Rohingya strike highlights growing refugee activism. The New Humanitarian. https://www.thenewhumanitarian.org/news-feature/2018/11/27/bangladesh-rohingya-strike-highlights-growing-refugee-activism

16   UNHCR. (2019). Operational Update—Bangladesh. https://data2.unhcr.org/en/documents/download/72444

17   BD News 24. (2019, September 3). BTRC orders telecom operators to stop services to Rohingyas in seven days. https://bdnews24.com/bangladesh/2019/09/02/btrc-orders-telecom-operators-to-stop-services-to-rohingyas-in-seven-days

18   Emont, J. (2019, September 3). Bangladesh Cuts Mobile Access to Rohingya Refugees. Wall Street Journal. https://www.wsj.com/articles/bangladesh-cuts-mobile-access-to-rohingya-refugees-11567541883

19   Rahman, Zara. (2015, December 22). Bangladesh will demand biometric data from all SIM card users. Global Voices. https://globalvoices.org/2015/12/22/bangladesh-will-demand-biometric-data-from-all-sim-card-users

20   McVeigh, Karen. (2019, September 5). Bangladesh imposes mobile phone blackout in Rohingya refugee camps. The Guardian. https://www.theguardian.com/global-development/2019/sep/05/bangladesh-imposes-mobile-phone-blackout-in-rohingya-refugee-camps

21   USA for UNHCR. (2019, February 7). Ethiopia Refugee Crisis Explained. https://www.unrefugees.org/news/ethiopia-refugee-crisis-explained

22   UNHCR. (2019). Global Trends—Forced Displacement in 2018. https://www.unhcr.org/globaltrends2018

23   Momodu, S. (2015, April). Refugees turn to Ethiopia for safety and asylum. African Renewal | UN. https://www.un.org/africarenewal/magazine/april-2015/refugees-turn-ethiopia-safety-and-asylum

24   UNHCR. (2018). Comprehensive refugee response framework: The Ethiopia model. http://www.globalcrrf.org/wp-content/uploads/2018/12/UNHCR-CS-Ethiopia-screen.pdf

25   UNHCR. (2018). Ethiopia Country Refugee Response Plan—The integrated response plan for refugees from Eritrea, Sudan, South Sudan and Somalia. https://data2.unhcr.org/ar/documents/download/62986

26   Bhalla, N. (2019, January 17). Ethiopia allows almost 1

million refugees to leave camps and work. Reuters. https://www.reuters.com/article/us-ethiopia-refugees-rights-idUSKCN1P-B2QH

27 UNHCR. (2018). UNHCR Strategy on Digital Identity and Inclusion. https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf

28 The World Bank. (2016). ID4D - Country Diagnostic: Nigeria. http://documents.worldbank.org/curated/en/136541489666581589/pdf/113567-REPL-Nigeria-ID4D-Diagnostics-Web.pdf

29 The World Bank. (2018). Project Information Document/Integrated Safeguards Data Sheet (PID/ISDS)—Nigeria Digital Identification for Development Project (p. 9). http://documents.worldbank.org/curated/en/501321536599368311/pdf/Concept-Project-Information-Document-Integrated-Safeguards-Data-Sheet-Nigeria-Digital-Identification-for-Development-Project-P167183.pdf

30 Novitske, L. (2019, July 31). Reaching the unbanked—MTN to shake up Nigeria's fintech sector. The Africa Report. https://www.theafricareport.com/15837/reaching-the-unbanked-mtn-to-shake-up-nigerias-fintech-sector

31 Bloomberg. (2019, September 20). Nigeria to Give All of Its 200 Million People Identity Numbers. Daily Maverick. https://www.dailymaverick.co.za/article/2019-09-20-nigeria-to-give-all-of-its-200-million-people-identity-numbers

32 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

33 Nwaogu, C., & Ihejirika, P. (2018, April 1). 28.5m Nigerians Agonise Over Suspension Of Nat'l ID Card Issuance. Leadership Newspaper. https://leadership.ng/2018/04/01/28-5m-nigerians-agonise-over-suspension-of-natl-id-card-issuance

34 Court, A. (2014, September 25). Branding Nigeria: MasterCard-backed I.D. is also a debit card and a passport. CNN. http://edition.cnn.com/2014/09/25/business/branding-nigeria-mastercard-backed-i-d-/index.html

35 Mhlanga, B. (2017, June 22). Zec, Nikuv BVR 'rigging' plot exposed. NewsDay Zimbabwe. https://www.newsday.co.zw/2017/06/zec-nikuv-bvr-rigging-plot-exposed

36 Kwaramba, F. (2017, August 31). Mudede metal ID ban triggers panic. DailyNews Live. https://www.dailynews.co.zw/articles/2017/08/31/mudede-metal-id-ban-triggers-panic

37 Majoni, T. (2017, October 13). BVR: The Zanu PF election cheat sheet. The Standard. https://www.thestandard.co.zw/2017/10/23/bvr-zanu-pf-election-cheat-sheet

38 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

39 Realising the value of this data, Zimbabwe pushed for a better contract, leading negotiations to stall and another Chinese company, Hikvision, to make an offer. No further updates on partnerships with the private sector have been made public. Details regarding this change can be found in https://www.bloombergquint.com/china/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain

40 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

41 Chutel, L. (2018, May 25). China is exporting facial recognition software to Africa, expanding its vast database. Quartz Africa. https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity

42 Ibid.

43 Ruhanya, P., & Gumbo, B. (2018, March 16). Militarisation of politics rarely delivers democracy. The Zimbabwe Independent. https://www.theindependent.co.zw/2018/03/16/militarisation-politics-rarely-delivers-democracy

44 MISA. (2018, September 15). Zimbabwe government steps up surveillance efforts. Media Institute of Southern Africa Zimbabwe. https://zimbabwe.misa.org/2018/09/15/zimbabwe-government-steps-up-surveillance-efforts

45 Thailand's first attempt at a digital ID system "to transform Thailand into a world leader of public service modernization" was riddled with problems. The government expected to register 64 million people in three years without conducting a pilot or feasibility study, relied on incompatible technologies, failed to provide clarity on how the card functioned and faced bureaucratic complications and accusations of corruption. See Gao, P., & Gunawong, P. (2014). Available at: http://hummedia.manchester.ac.uk/institutes/gdi/publications/workingpapers/igov/igov_wp23.pdf

46 Theparat, C., Chantanusornsiri, W., & Banchongduang, S. (2018, September 12). Cabinet gives nod to draft digital ID bill. Bangkok Post. https://www.bangkokpost.com/thailand/general/1538174/cabinet-gives-nod-to-draft-digital-id-bill

47 Pornwasin, A. (2018, September 16). Mixed reactions to Digital ID draft law. The Nation Thailand. https://www.nationthailand.com/national/30354611

48 Kitiyadisai, K. (2004). Smart ID Card in Thailand from a Buddhist Perspective. Manusya: Journal of Humanities, 7(4), 37–45. https://doi.org/10.1163/26659077-00704003

49 Augn, N. L. (2016, March 1). Workers in Thailand told to re-register for pink cards. The Myanmar Times. https://www.mmtimes.com/national-news/19233-workers-in-thailand-told-to-re-register-for-pink-cards.html

50 At the time of writing (November 2019) this amount was equivalent to EUR 750.

51   Bratton, M., & Masunungure, E. V. (2018). PP47: Public attitudes toward Zimbabwe's 2018 elections: Downbeat yet hopeful? | Afrobarometer. Afrobarometer, Policy Paper No. 47. https://afrobarometer.org/publications/pp47-public-attitudes-toward-zimbabwes-2018-elections-downbeat-yet-hopeful

52   See the case studies in the Annex for further details on what each system is designed to achieve.

53   In response to a draft of this report, UNHCR told us that "protecting refugees' personal data is an essential part of refugee protection. The organization adopted, as early as 2014, a Policy on the Protection of Personal Data of Persons of Concern to UNHCR and appointed a Senior Data Protection Officer to support its implementation across its programmes globally".

54   For more information on the rights discussed here, see the United Nations Universal Declaration of Human Rights. Available at: https://www.un.org/en/universal-declaration-human-rights

55   See, for example Fortify Rights at https://www.fortifyrights.org/ and Arakan Rohingya National Organisation at https://www.rohingya.org

56   Freedom House. (2019, February 2). Ethiopia: Civil Society Proclamation Advances Essential Freedoms. https://freedomhouse.org/article/ethiopia-civil-society-proclamation-advances-essential-freedoms

57   UNHCR. (2018). Chapter 4—Guidance on Registration and Identity Management. In Guidance on Registration and Identity Management. https://www.unhcr.org/registration-guidance/chapter4

58   Oakeshott, N., Marskell, J., Chapman, E. W., & Benihirwe, M. (2018, June 19). Empowering refugees and internally displaced persons through digital identity. UNHCR Blog. https://www.unhcr.org/blogs/empowering-refugees-internally-displaced-persons-digital-identity

59   The World Bank. (2018). Project Information Document/Integrated Safeguards Data Sheet (PID/ISDS)—Nigeria Digital Identification for Development Project (p. 9). http://documents.worldbank.org/curated/en/501321536599368311/pdf/Concept-Project-Information-Document-Integrated-Safeguards-Data-Sheet-Nigeria-Digital-Identification-for-Development-Project-P167183.pdf

60   UNHCR's guidance on taking photographs says, "Head coverings, hair, head-dress or facial ornaments should not obscure the face". See UNHCR. (2018). Chapter 5.2 Registration as an Identity Management Process -. In Guidance on Registration and Identity Management https://www.unhcr.org/registration-guidance/chapter5/registration

61   At the time of writing (November 2019), this amount was equal to EUR 1.25.

62   Nigeria National Identity Management Commission. (2018, April 5). Modification of Names Available at NIMC Offices Nationwide. https://www.nimc.gov.ng/modification-of-names-available-at-nimc-offices-nationwide

63   UNHCR. (2018). Chapter 8.2—Continuous registration in UNHCR Operations. In Guidance on Registration and Identity Management. https://www.unhcr.org/registration-guidance/chapter8/continuous-registration-in-unhcr-operations

64   UNHCR. (2018). Guidance on the protection of personal data of persons of concern to UNHCR. https://www.refworld.org/pdfid/5b360f4d4.pdf

65   EUGDPR. (n.d.). Key Changes with the General Data Protection Regulation. https://eugdpr.org/the-regulation

66   Regarding this statement, the guidance cites the 2017 Handbook on Data Protection in Humanitarian Action by the International Committee of the Red Cross, which as of October 2019 announced significant changes to their biometric policies and procedures, enabling refugees to have control over their data and to refuse biometrics without facing consequences. For more information, see Hayes, B., & Marelli, M. (2019, October 18). Facilitating innovation, ensuring protection: The ICRC Biometrics Policy. Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy

67   Weindling, P. (2001). The origins of informed consent: The International Scientific Commission on Medical War Crimes, and the Nuremberg code. Bulletin of the History of Medicine, 75(1), 37–71. https://doi.org/10.1353/bhm.2001.0049

68   Knifed, E., Lipsman, N., Mason, W. & Bernstein, M. (2008, June). Patients' perception of the informed consent process for neurooncology clinical trials. Neuro Oncology, 10(3), 348–354.

69   Of the sites we explored, Ethiopia, Nigeria and Zimbabwe are parties to the Convention. See UNHCR. States Parties to the 1951 Convention relating to the Status of Refugees and the 1967 Protocol. https://www.unhcr.org/protect/PROTECTION/3b73b0d63.pdf

70   Ahmed, K. (2018, November 27). In Bangladesh, a Rohingya strike highlights growing refugee activism. The New Humanitarian. https://www.thenewhumanitarian.org/news-feature/2018/11/27/bangladesh-rohingya-strike-highlights-growing-refugee-activism

71   Hayes, B., & Marelli, M. (2019, October 18). Facilitating innovation, ensuring protection: The ICRC Biometrics Policy. Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy

72   Designed in 2015, BIMS, or the Biometric Identity Management System, is part of UNHCR's digital Population Registration and Identity Management Ecosystem (PRIMES). More information about BIMS is available at https://www.unhcr.org/en-us/protection/basic/550c304c9/biometric-identity-management-system.html

73   UNHCR. (2018). Chapter 5.2 Registration as an Identity

Management Process -. In Guidance on Registration and Identity Management. https://www.unhcr.org/registration-guidance/chapter5/registration

74   Kaurin, D. (2019). Data Protection and Digital Agency for Refugees. WRC Research Paper No. 12. World Refugee Council Research Paper Series. Centre for International Governance Innovation. https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees

75   Latonero, M., Hiatt, K., Napolitano, A., Clericetti, G., & Penagos, M. (2019). Digital Identity in the Migration & Refugee Context—Italy Case Study. Data&Society. https://datasociety.net/output/digital-identity-in-the-migration-refugee-context

76   European Union agencies use EURODAC to match fingerprints. See more at https://ec.europa.eu/knowledge4policy/dataset/ds00008_en

77   Good ID. (2019). Report—Good ID: What's trust got to do with it? https://www.good-id.org/en/articles/good-id-whats-trust-got-to-do-with-it-workshop-report

78   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

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

80   Bangladesh Parliament. Digital Security Act of 2018. , Pub. L. No. Act No 46 of the Year 2018 (2018). https://www.cirt.gov.bd/wp-content/uploads/2018/12/Digital-Security-Act-2018-English-version.pdf

81   Amnesty International. (2018, September 20). Bangladesh: New Digital Security Act imposes dangerous restrictions on freedom of expression. https://www.amnesty.org/en/latest/news/2018/09/bangladesh-new-digital-security-act-imposes-dangerous-restrictions-on-freedom-of-expression/

82   Thailand National Authorities. (2015). Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act. Translated byThai Netizen Network. https://thainetizen.org/wp-content/uploads/2015/01/personal-data-protection-bill-20150106-en.pdf

83   Ethiopia National Authorities. (2019, February 27). Ethiopia: Proclamation No. 1110/2019. https://www.refworld.org/docid/44e04ed14.html

84   BenarNews. (2019, July). Bangladesh Gives Myanmar 25,000 Rohingya Names for Potential Repatriation. Radio Free Asia. https://www.rfa.org/english/news/myanmar/bangladesh-refugees-07292019172753.html

85   To be clear, UNHCR has policies against sharing data with countries of origin.

86   The names and details of some groups have been left out for security purposes.

87   UNHCR noted that they also use the language of 'registration' in addition to 'verification' and provides guidance on communicating about such issues, available here: https://www.unhcr.org/registration-guidance/chapter4

88   ID2020 | Digital Identity Alliance. https://id2020.org

89   Rahman, Z. (2016, November 21). Dangerous Data: The role of data collection in genocides. The Engine Room. https://www.theengineroom.org/dangerous-data-the-role-of-data-collection-in-genocides

90   Ahmed, K. (2018, November 27). In Bangladesh, a Rohingya strike highlights growing refugee activism. The New Humanitarian. https://www.thenewhumanitarian.org/news-feature/2018/11/27/bangladesh-rohingya-strike-highlights-growing-refugee-activism

91   Namati. (n.d.). Stopping the Digital ID Register in Kenya – A Stand Against Discrimination. https://namati.org/news-stories/stopping-the-digital-id-register-in-kenya-a-stand-against-discrimination

92   Chima, R. J. S., Aggarwal, N. M., & Singh, A. K. (2018, September 26). Supreme Court of India rules to restrict world's largest digital identity framework (Aadhaar)—But debate continues. Access Now. https://www.accessnow.org/supreme-court-of-india-rules-to-restrict-worlds-largest-digital-identity-framework-aadhaar-but-debate-continues

93   Sayadi, E. (2018, January 11). Biometric ID vs. privacy: Tunisians win on privacy! But it's not over yet. Access Now. https://www.accessnow.org/biometric-id-vs-privacy-tunisians-stood-privacy-not-yet

94   Mzalouat, H. (2018, March 22). Carte d'identité biométrique: Chronique d'un projet de loi avorté. Inkyfada. https://inkyfada.com/fr/2018/03/22/carte-identite-biometrique-tunisie

95   Digital Watch Observatory. (2019, April 13). Supreme Court declares Jamaica Digital ID unconstitutional. Geneva Internet Platform. https://dig.watch/updates/supreme-court-declares-jamaica-digital-id-unconstitutional

Annex A
Methodology

In early 2019 we recruited in-country researchers for each site, ensuring that each researcher had both lived and contextual expertise of the sociopolitical context in which the system was situated. We used existing relationships and networks to identify researchers and put more emphasis on their position and lived experience than on their technical expertise or formal research credentials.

In some cases, the researchers were, or will be, subject to the very digital ID systems they were studying. We saw close proximity to systems and people affected as a benefit – one which would allow for deeper levels of insights to emerge. This was intentional, as we aimed to take an alternative approach to that which we commonly see being carried out in this field, where researchers from the Global North make brief visits to other countries and come away with insights that either lack or include a limited amount of local knowledge and expertise. Working with in-country researchers who have a deep understanding of the targeted communities provided richer, more nuanced insight.

Given our objective of prioritising locally led research, we used participatory design and brought the researchers together in remote calls with The Engine Room's programme staff and a research design consultant to jointly develop a research framework for the overall project. We wanted to ensure that while the overarching objectives of their work were the same,

the methods for reaching those objectives integrated the researchers' respective experience and knowledge.

The end framework identified four key lines of inquiry:

1   **The digital ID system: How it is/was planned and how it functions**

2   **People's lived experience: Where they encounter the system and feel its effects**

3   **People's 'unknown' experience: Where the system affects them in ways they may not be directly aware of**

4   **Civil society: Current and potential engagement**

The methodology included a literature review, in-depth expert interviews, civil society mapping and interviews, sampling and selection of target groups, and focus groups. Each researcher then took these methodologies and adapted them for their local context, a critical step because we wanted to ensure that the project considered such factors as power imbalances, cultural norms, histories of trauma and political maneuvering that local researchers would recognise more easily than outside researchers. To maintain the integrity of the research process, we worked with a participatory research consultant who provided group and individual support to the researchers as they adapted methodologies. More information about methodologies in each location can be found in the case studies in the annex.

Our internal team also contributed to the literature review, which focused on official documentation, studies and reporting related to the selected systems and their contexts, as well as a broader review of literature on other national-level and humanitarian systems, best practices for digital ID, identity and human rights, data protection, privacy and surveillance.

Interviews and focus group discussions ran from late February to May of 2019. In-depth expert interviews focused on key stakeholders involved in the design and implementation of each digital ID system, e.g., government officials, aid agency representatives, partners and experts. In total, the researchers interviewed 33 of these key informants.

In-country researchers were able to identify civil society organisations through the literature review, expert interviews and their own knowledge, and then used a snowball method to expand. They each identified civil society groups addressing the needs of marginalised people, such as women, LGBTQI folks, disabled people, sex workers, elderly people, rural farmers, Indigenous people and migrants. Semi-structured individual interviews and group discussions were held with civil society organisations that are actively engaged on issues around digital ID and those concerned but not yet engaged. Because civil society representatives were often users of the systems being examined, researchers were able to pilot 'lived experience' focus groups in these settings.

With individuals affected by each system, the aim was for a deep dive into experiences, especially of groups that are particularly vulnerable to the negative effects of digital ID, rather than a representative sample of the general population. For this reason, we also used outlier case sampling.[1] Target groups were identified through the literature review and interviews with expert stakeholders and civil society. In total, there were 29 focus groups of civil society representatives and people experiencing digital ID systems plus 22 one-on-one interviews with the latter population. Overall, we spoke to more than 100 people targeted by the selected digital ID systems in addition to civil society representatives.

We encouraged researchers to use participatory tools, such as visual and verbal cues for exploration and scenario-based activities. These methods were easier in some settings than others. For instance, researchers in Zimbabwe were able to use visuals made by local artists and   spark discussion around several scenarios because of their close proximity to the

communities, but in Ethiopian camps, where translation was necessary and access and time were limited, it was easier to do more traditional interviews.

Additionally, we gave researchers templates for discussing the purpose of the research and how the data would be used and protected as well as obtaining consent. In each site consent was given in writing or verbally. Participants were also given the opportunity to opt-out at any point, and researchers checked consent again at the end of focus groups. While financial incentives were not given to participants, some researchers provided refreshments and local travel reimbursement in accordance with local practice.

Notes

1   Outlier (or extreme, or deviant) case sampling means focusing on special or unusual cases that highlight notable successes or failures. These cases offer insight into the experiences of marginalised people, anticipate trends that might eventually reach the mainstream and provide lessons for future work.

Annex B

Digital ID in Bangladeshi

Refugee Camps: A Case Study

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 researcher in Bangladesh put together a local team to overcome language and cultural barriers to communication with the Rohingya Muslim population. The team involved both male and female research assistants and interpreters, as well as translators to convert transcripts into English.

The research in Cox's Bazar consisted of ten in-depth interviews with key informants amongst the Rohingya refugee community, such as majhis[1] and other community leaders, and a senior official from the Bangladeshi Government's Refugee Relief and Repatriation Commission (RRRC), and ten focus groups with Rohingya sub-communities, including especially vulnerable groups such as people with disabilities, elderly people, women whose husbands had been killed by the Myanmar Army and survivors of torture by the Myanmar Army. This primary research was conducted in Ukhiya and Teknaf camps between March and April 2019. All quotations from refugees and key informants come from in-person interviews and discussions during this period in Cox's Bazar. More information on the methodology can be found in the global report.[2]

Repeated failed attempts to enter the camps in Cox's Bazar forced the research team to work more quickly than planned once they finally obtained permission. Lengthy waits for interviews once inside the camps also slowed work down. While the team had success putting focus groups together and interviewing community leaders and representatives of the Bangladeshi government, no UNHCR staff working in Bangladesh agreed to an interview. While writing the research outputs (in November and December of 2019), we reached out to UNHCR's Division of Programme Support and Management for comments, which we have included here.

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 that are not designed to address diversity of experience and identity.

Historical Context

In 2017 after decades of persecution (including the refusal of recognition in identification documents since 1982), more than 700,000 Rohingya Muslims fled Myanmar due to targeted violence carried out by the military (which controls all security forces, law enforcement and certain government positions) in what UN investigators have called an operation executed with "genocidal intent".[3] Individuals and families fled to neighbouring countries, the majority to Bangladesh, where the government agreed to shelter the Rohingya on the condition of the refugees eventually returning to Myanmar. Approximately 900,000 Rohingya refugees are in Bangladesh as of August 2019.[4]

The role of government-issued ID in the Rohingya case is particularly sensitive, given that the violence against them is specific to their identity. The Myanmar government does not recognise Rohingya Muslims as an ethnic people of Myanmar (although it officially recognises several other groups), and many are not granted citizenship despite being born in the country. As such, in contrast to many other 'best practice' cases of either not collecting data

Rohingya camps in Cox's Bazar, Bangladesh

on ethnicity or not displaying it on ID cards, the Rohingya have demanded that their ethnic identity be explicitly acknowledged on identification documents. Including their ethnicity on IDs is, for them, a key step toward ensuring that their ethnic identity is acknowledged and their Myanmar citizenship is granted and preserved.

Multiple types of identification systems are in use with this population. We looked at the UNHCR registration process (locally known as 'joint verification process' or 'smart card project'), but for context, we also describe here the official identification documents offered to (or by many accounts, forced upon[5]) the Rohingya by the Government of Myanmar since 2016,[6] known in its latest iteration as the "National Verification Card" (NVC).

The NVC effectively identifies Rohingya people as "foreigners", omitting their Rohingya identities, and denying them citizenship and associated rights. Critics say that the Government of Myanmar will use the system to track the Rohingya population, with potential for further targeted persecution.[7] Rohingya refugees we spoke to say they will feel confident this information will not be used against them only if citizenship is granted alongside data collection.

But in this scheme, their citizenship is denied; thus, many Rohingya are refusing both to return to Myanmar and to claim NVCs. This leaves them at somewhat of a standoff: the Myanmar government say that accepting the NVC is a condition of repatriation, and the Rohingya refuse to accept the NVC without also receiving citizenship. As an imam interviewed as part of this research said:

There's a reason behind the Rohingya identity we are looking for. The [different] ethnicities in Myanmar, all of them get the citizenship on the basis of their racial identity... They gave all the ethnic people their ethnic identity but they didn't give us [the Rohingya] that. All the people from different ethnicity had the freedom of movement but not us. All the facilities of Burma depend on the ethnic identity. That's why we tell everyone to give us the nationality with ethnicity.

A report released by Rohingya rights group Fortify Rights in early September 2019[8] documents incidents where Rohingya Muslims in Myanmar were held at gunpoint and forced to accept NVCs, quoting Rohingya people as saying: "The document that you have to fill out for the NVC makes us feel shame. It says we are outsiders". This statement highlights the way in which both the end product of the identification system and its process affect the dignity and rights of the people subjected to the system. The report includes another instance in July 2017:

... Myanmar Army soldiers and government officials entered Baw Tu Lar village—also known as Bandola village—in Rakhine State's Maungdaw Township and forced groups of Rohingya to accept NVCs, in some cases at gunpoint. "[The soldiers] closed the door and surrounded us, holding guns," a Rohingya man, 61, told Fortify Rights. Myanmar authorities forced him and four of his seven family members to accept the NVC. "They separated men and women... The threats to receive an NVC are real. It's a horrible situation for us".[9]

Rohingya camps in Cox's Bazar, Bangladesh

The Digital ID System

Since June 2018, the Bangladeshi government and the United Nations High Commissioner for Refugees (UNHCR), has carried out a joint registration exercise aimed at collecting personal data and issuing ID cards to Rohingya refugees who fled Myanmar for Bangladesh in response to Myanmar military operations in predominantly Rohingya areas. This exercise is "for the purposes of protection, identity management, documentation, provision of assistance, population statistics and ultimately solutions for an estimated 900,000 refugees".[10] As of August 2019, an average of 5,000 refugees were being registered each day at seven sites within the settlements at Cox's Bazar.[11] UNHCR staff collect iris scans, fingerprints and family information, and smart cards connected to this data are issued by UNHCR and the Government of Bangladesh.

After the Bangladeshi government's failed repatriation efforts in which no Rohingya refugees volunteered to return to Myanmar, the government reportedly began sharing refugee data[12] with the Myanmar government. In July 2019, a list of 25,000 Rohingya people was handed over to Myanmar,[13] and reports on social media[14] suggest this data included paper copies of photographs and fingerprints, though the claim remains unconfirmed. In total, according to Bangladeshi media, the government has given three lists containing names of 55,000 Rohingya to the Myanmar government.[15]

We have found no evidence of a tripartite voluntary repatriation agreement[16] between Myanmar, Bangladesh and UNHCR. Theoretically, such an agreement would clarify the data sharing arrangements, including what data is shared with the Myanmar government and how this sharing happens, but at the time of writing, no such agreement has been publicly shared or confirmed. Instead, UNHCR has been working under separate memoranda of understanding with each government.[17]

Lived Experiences

The interviews and focus groups that we conducted in Cox's Bazar in March-April 2019 shed light on the lived experience of refugees interacting with the registration system led by UNHCR and the Government of Bangladesh. 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 refugees do not have one unified experience. Some of the experiences described in this case study may contradict official reports or UNHCR and Bangladeshi government guidelines.** We aim for these learnings to become part of the broader discussion on digital ID solutions in humanitarian contexts.

Outreach and information provision

Despite UNHCR's guidance on community engagement,[18] the refugees we interviewed reported that information provision around the scope and purpose of the digital ID system was sparse and inconsistent. Information was distributed to community leaders, who then shared details with their communities. Our interviews show that women were the last to be informed – frequently third-hand via men and boys in their community. In a focus group with women living with disabilities, one participant said, "They had discussions with males. Those who have boys in their families, they were able to go".

The Office of the Refugee Relief and Repatriation Commissioner (RRRC) of Bangladesh made an effort to clarify misunderstandings about the card but, from what we were told, not until they were affecting enrolment rates. As the commissioner at the time said, "They were having doubts… We tried to encourage them by doing a lot of focus group discussion or repeated sessions… We tried to make them understand that it's for their own good". Some of the refugees we spoke to do not trust information from the RRRC and UNHCR and look instead to the diaspora community for advice and information. A protest leader said:

> The day before going to the office, we gave a picture of this card in the Facebook to some of the leaders of ours, who live abroad, to get suggestions. Then the next day we went to the office of [a Rohingya rights group]. They told us not to take it and the leaders of ours, who live abroad also told us not to take it.

In addition, language barriers posed a challenge for some refugees. Smart cards issued to this population are written in English and Bengali. Refugees who are not literate[19] or do not know how to read English or Bengali do not know what is written on their IDs.

When asked what is written on the smart card, one participant replied, "How can we tell brother? We can neither read English nor can we read Bengali." Another said, "What could be written there? They are not supposed to write that we are Bangladeshis, right? They may write that we are from Burma. Since we cannot read, we do not know".

Refusing to register – Protest in November 2018

Not long before our field research in Cox's Bazar, refugees staged a protest against UNHCR's ID system and refused to register. Protest leaders told us that this refusal was due to the fact that the ID cards do not identify individuals as "Rohingya". As one majhi told us, "If they listed us as Rohingya Muslim, [refugees] will participate in the data [collection]. Otherwise, they won't. People were afraid. They said, they will not give us Rohingya, how can we give [data]?"

For many Rohingya refugees, this problem mirrors the erasure of identity that refugees faced in Myanmar with the NVC. As one interviewee said, "We think NVC card is the elder sibling and smart card is its younger sibling. Both come from the same root… that is what we think. If this happens, we will still be considered as foreigners in our own country".

Over several days, discussions between system administrators and community and protest leaders resolved the situation. After administrators shared more information about the purpose of the smart card and explained that ethnicity was logged in the database, even if not displayed on the card itself, protesters were convinced to end their demonstration and registration continued. The RRRC described the response:

> They wanted to mention Rohingya ethnicity on the card but we tried to make them understand that the ethnicity is never mentioned in any identity or identification card… it's not necessary here… In the main database we are including their ethnicity as being a Rohingya… After seeing that they believed or got convinced that it's fine…

Awareness and understanding

People we interviewed said there was little shared understanding of the purpose of the digital ID system across actors, administrators and users of the system. In addition to reducing fraud[20] – "misuse by duplicating these identifications" – the RRRC said the card serves the purpose of "separating them from our own population" and to support repatriation efforts "when the condition of Myanmar [improves]". One refugee said he was told that the card means they are "UNHCR's responsibility now" and equates refugee status with possessing smart card: "Now UNHCR has given you the cards and they will let the world know that you will be now officially regarded as refugees." Another refugee talked of how "we need everyone's biodata to know how many Rohingyas came here".

Multiple participants spoke of fears around data sharing with Myanmar. "We are still having doubts about one matter… they assured us that they won't share our biodata with the [Government of Myanmar], but what if they cheat us and share this data… [and] send us back to [Myanmar]?"

Most often, when asked about the ID's purpose, people equated it with getting rations or receiving aid, something explored more below in the section on informed consent. For many interviewees, the smart card was seen as preferable to the old system, as it means having only one card, rather than different cards for different kinds of rations: "Previously they would give us so many cards… for rice, pulses, healthcare, kerosene… But for all these, there is only one card now".

Refugees displayed low levels of understanding about the purpose of the biometric component of the digital ID system and of the consequences of a potential data breach. Interviewees and focus group participants often had conflicting ideas about the purpose of biometrics, ranging from viewing it as a standard UNHCR practice (with no more detail than that) to

being told the iris scanners were checking for eye disease. If the latter claim is true, this is significant misinformation that violates informed consent.

- "I asked them, 'why are you scanning our iris? Government didn't do such a thing.' They told us that, 'it is being done on behalf of UNHCR'".
- "They told me that, 'UNHCR scans the iris of the refugees everywhere in the world'".
- "They told me that they are checking our eyes to know if we have any eye disease".
- "They did something to our eyes using a large pipe. Yes. They did something. I could see another pair of eyes there".

When asked about the purpose of biometrics in the digital ID system, the RRRC felt that any concerns were invalid as this population had already been discriminated against without their biometrics. The commissioner said,

> Without this biometric data, they were being tortured before... If they want to torture them, if they want to harm them, biometric data is not an issue over there, isn't it? If I want to discriminate among a population, I don't need their biometric data... As they were already being tortured in a vicious cycle from the late 70s... Biometric data didn't play any role on that...So, they're afraid of being just nothing, it's unnecessary.

This idea perpetuates a cycle of experimentation[21] on vulnerable communities and restricts refugee agency and dignity. Treating forcibly displaced people better than their countries of origin do is a low bar and does not align with the tenets of the 1951 United Nations Convention Related to the Status of Refugees,[22] though Bangladesh is not a signatory. The Commissioner's comment does, however, align with the views of several refugees we interviewed who said their impoverished circumstances were so severe that worrying about biometric data was secondary to their needs for food, shelter and physical safety.

Lack of informed consent

UNHCR policies[23] require that digital ID systems be deployed with the informed consent of all people registering into these systems. In other words, all registrants should understand the purpose and scope of the system. As such, inconsistent understanding around the purpose of this system may reflect problems with the implementation of the informed consent policy.

An activist leader reported that individuals were not asked for consent to capture biometric data but that UNHCR or government staff held meetings camp by camp to inform people that they "would like to collect your data… It is useful, not for us, but for you". He added, "When people are going there at the center, they already understood – he is agreed and he has understood". Because focus group participants described being informed about the smart card by majhis and other community leaders, we asked for clarification. The activist leader confirmed that UNHCR or government staff met with leaders, not everyone: "Everybody was not included, but the most important persons were included". What interviewees described then was a tiered process where community leaders indirectly gave group consent rather than staff going through UNHCR's informed consent process[24] for each individual at registration.

Interviewees reported to us that system administrators told refugees that registering with the system was a requirement for receiving aid. In this context, refugees cannot refuse to register, as they cannot survive without rations. One said: "They told that it is compulsory to take the smart card otherwise we won't get rations… Then we didn't have any other options but taking the card".

Having viable alternatives is a necessary and critical part of providing a service where people's right to consent is respected. Moreover, vulnerable populations operating in survival mode often do not have the privilege of considering the consequences of sharing their per-

sonal data. An activist pointed out that they do not fear what will happen with their biometrics; they are "just afraid of the Myanmar". When asked who might do harm with their information, a focus group participant responded, "We live in a house made of tarpaulin. It is so hot there that any such question never crosses our mind".

Some refugees were so grateful to the Bangladeshi government for their aid that they put full trust in them to collect any desired information: "The things that Bangladeshi people did for us; we will never forget that. We will never be able to repay them. We will obey the Bangladesh government. If they even sell us, we won't say anything because they saved us from death". This is another example of the power imbalance at play, reflecting how easy it can be for those in power to push through systems without considering refugee rights and dignity. As another refugee stated, "We are not actually taking it willingly. We are taking it since we are under your rule now; we must follow the laws of your country".

Interestingly, many of the refugees we spoke to did not trust UNHCR, referring to the refugee agency as a "liar" and "trickster" due to its apparent allegiance with Myanmar and that government's NVC. An imam reported:

> We are not scared of the Bangladeshi government. We are scared of the UNHCR… In June 2018, UNHCR signed an MoU with the Government of Myanmar. On the basis of that deal, the UNHCR requested us to [register for] the NVC card. So, we can see that the UNHCR is also trying to make us foreigners.

This lack of trust contributed in part to refugees' refusal to register for smart cards: "…but then we saw the logo of UNHCR in the smart card, for which all of these problems were being created. If UNHCR's logo wasn't there, then there would not be any problem at all". This negative perception also has a ripple effect on NGOs and other civil society organisations. The same imam stated:

Every NGO is talking about this smart card, but UNHCR is the agent of all NGOs. That's why they control the information of the other NGOs... all the NGO is trying to do business by us. They don't think about our good. Not a single NGO wants our good. They just want their own development... all the NGO follow UNHCR. Where UNHCR doesn't want our good, then why would other organizations want our good? ...We told them so many times to work for our rights, but they aren't doing it.

The stark contrast to refugee trust in the Bangladeshi government reflects their lack of information about the relationship between Bangladesh and Myanmar. Without adequate, accessible information about ongoing talks between these two governments, refugees are left to make assumptions about their motives and interests. While this kind of problem is likely not unique to the Rohingya context, it appears to make it difficult for UNHCR and other aid and civil society organisations to be fully effective.

Rohingya camps in Cox's Bazar, Bangladesh
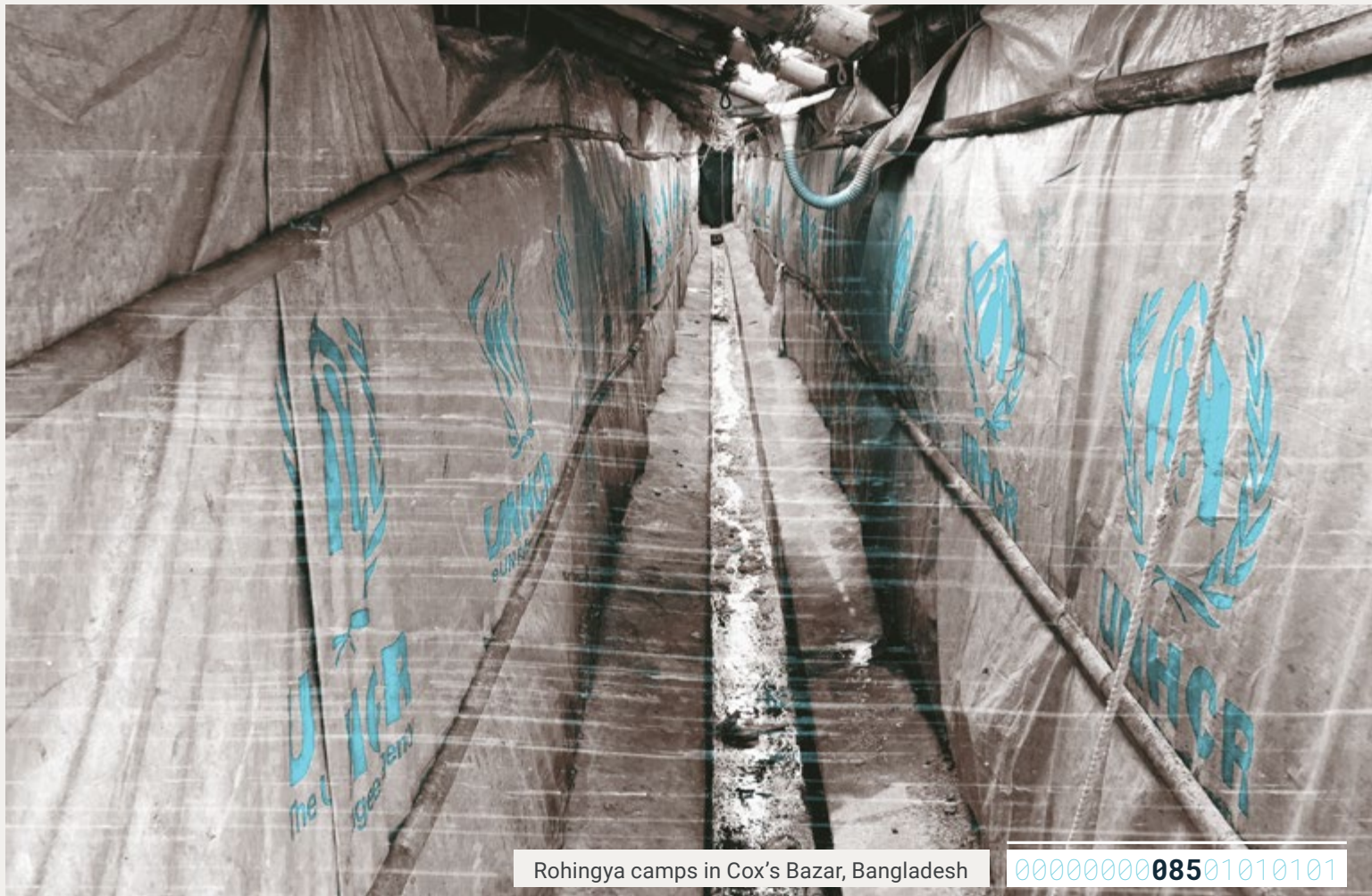
Problems during the registration process

In addition to what appears to be a lack of informed consent, the refugees we spoke to detailed other problems with the joint verification process. Some mentioned having to stand or wait for long periods of time, with multiple interviewees waiting in line for more than five hours. One imam we spoke to described the scene:

> [T]hey call more people to do the smart card than is possible in one day. After going there, people stand there the whole time. Those who can't do the smart card, go back home and face the same trouble the next day when they go to do the smart card again. If people get stuck in the crowd, volunteers take money from them and take them to the front to do the smart card. To take money… is against the rules.

We observed multiple registration centres and saw that the waiting areas were often very congested and uncomfortable due to heat, cramped conditions and lack of seating for those in need such as pregnant women, children and disabled people.

Furthermore, the registration process did not consistently respect cultural norms. Women reported having to remove head scarves and jewelry, an experience that some described as "humiliating". One woman who had to move her scarf back from her head said, "It felt bad… I was disrespected there which made me upset". Another reported:

> They opened our earrings and nose pins. They took the information by moving the cloth from our head, in naked head. Is this a way to do it by humiliating us? …If they wouldn't have done it in this way, it would have felt much better.

Post-research developments

Marking the second anniversary of the day targeted violence against the Rohingya began in Myanmar, more than 200,000 refugees gathered in a peaceful protest in Cox's Bazar on August 25, 2019.[25] During the same week, the Bangladeshi government made a second attempt to repatriate Rohingya refugees, but not a single person volunteered to return to Myanmar. Following this rally, the Bangladeshi government took a number of drastic actions, including:

- Removing the government official overseeing Bangladesh's response to the Rohingya, Refugee Relief and Repatriation Commissioner Mohammed Abdul Kalam, from his position[26]
- Banning all operations of 41 non-governmental organisations in the Rohingya camps
- Banning operations of two international NGOs operating in Cox's Bazar[27]

In addition, the government also took the unprecedented move of ordering telecommunications companies to block mobile phone access to Rohingya camps.[28] The government had imposed a ban on selling SIM cards to Rohingya refugees in 2017,[29] but the ban had not been strictly observed by telecommunications companies. Mustafa Jabbar, Bangladesh's minister of telecommunications, said publicly that this move "was prompted by Rohingya refugees' lack of proper identification documents, which means that by law they aren't allowed to register for SIM cards".[30] In 2016 Bangladesh introduced mandatory biometric registration for all SIM card owners, and set up a system where the fingerprints of individuals registering for SIM cards are verified against National ID cards (NIDS), enabling each SIM card to be traced to a single person.[31]

The telecommunications shutdown brings a new dimension to how technology and identification are used as tools of targeted exclusion. By ordering the Bangladesh Telecommunication Regulatory Commission (BTRC) to "verify mobile users in the camps"[32] within seven days of the order and forcing telecommunications operators to disable 3G and 4G internet to the camps, the Bangladeshi government took a drastic move against freedom of expression

and access to the internet with a strategy that combines governmental and corporate pow-ers. BTRC officials confirmed[33] that 3G and 4G access has been suspended indefinitely, while 2G (which allows for voice connectivity, but effectively no internet) remains operational.

It remains unclear whether telecommunications companies will follow the order to "deacti-vate" SIM cards in technical terms. Bengali-language media speculated in early September 2019 that one possibility could be that telecommunications companies share a list of active SIM cards in the camps with the government, which can then check those SIMs against a list of 'verified' SIM cards, ordering companies to deactivate any not on that list.[34]

The Bangladeshi government says these measures are being carried out in the name of "na-tional security",[35] but the move has faced Rohingya and international criticism[36] from media outlets, human rights groups and other governments that believe further isolation of Rohing-ya Muslims is not an effective solution.

A woman taking part in the process of making voter and national ID cards in Bangladesh

Conclusions and Recommendations

Considering the Bangladeshi government's response to a peaceful protest, it is more important than ever that civil society organisations working on digital rights connect with those supporting Rohingya refugee rights to share knowledge and strengthen advocacy efforts. The Engine Room plans to facilitate additional research with the Rohingya refugee community in Cox's Bazar and will continue to share findings and make connections between individuals and organisations addressing these challenges.

We encourage UNHCR to provide strong checks for ensuring that their informed consent policy is followed in the field. Critically, each person going through the verification process should understand what biometric data is being collected and how it will be used. Regardless of communication between UNHCR and community leaders, and then between those leaders and their communities, UNHCR's informed consent protocol should be followed with every individual at the time of registration. With regard to information provision, particular attention should be focused on language barriers, exploring ways of communicating the scope

of the system and the information on the smart card verbally or pictorially.

While the informed consent process remains vital, we cannot ignore the fact that refugees are rarely in a position to concern themselves with data privacy because, as several mentioned in focus groups, the burden of the violence they escaped and still fear, along with their need for basic necessities from the very institution requesting their data, weighs heavily on them. That Rohingya refugees in Cox's Bazar initially protested the smart card is unique among refugee camps and appears to be entirely due to their desire to have their ethnicity clearly recorded as a way to protect their Myanmar citizenship and avoid further persecution upon repatriation rather than any concerns about biometric data and camp power dynamics. These actions show that refugees can wield some power when banding together in fear for their lives, but at an individual level there is no way to push back.[37]

The Engine Room is committed to exploring how to resolve problems with informed consent. We recommend that decision makers and developers of digital ID systems consider alternatives that acknowledge power dynamics and maintain the dignity and rights of refugees, and we urge civil society to advocate for alternatives. This could involve inviting diverse representatives of newly displaced populations to give input on systems at various stages, improving information provision and grievance reporting processes to identify priorities, developing meaningful alternative processes that enable refugees to make choices, and revising information management processes.

Rohingya refugees have repeatedly been stripped of their agency and dignity, which makes it all the more important that they have opportunities to make decisions about their lives going forward. Given their lack of trust in UNHCR and apparent faith in the Bangladeshi government, which is reportedly sharing their data with Myanmar, a focus on awareness of the purpose, scope and risks of smart cards and biometric data collection is critical.
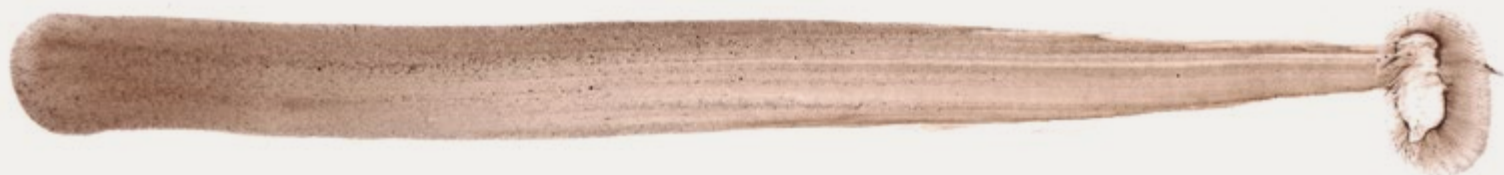
Notes

1   Rohingya community leader who is responsible for 80-120 households.

2   The Engine Room. (2020). Understanding the lived effects of digital ID: A multi-country report.

3   Office of the High Commissioner for Human Rights. (2019). Human Rights Council—Sexual and gender-based violence in Myanmar and the gendered impact of its ethnic conflicts. https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/sexualviolence/A_HRC_CRP_4.pdf

4   UNHCR. (2019). Rohingya Refugee Response—Bangladesh: Population factsheet. https://data2.unhcr.org/en/documents/download/71171

5   Fortify Rights. (2019). Tools of Genocide—National Verification Cards and the Denial of Citizenship of Rohingya Muslims in Myanmar. https://www.fortifyrights.org/downloads/Tools%20of%20Genocide%20-%20Fortify%20Rights%20-%20September-03-2019-EN.pdf

6   Ibid.

7   Ibrahim, A. (2019, August 1). Myanmar Wants to Track Rohingya, Not Help Them. Foreign Policy. https://foreignpolicy.com/2019/08/01/myanmar-wants-to-track-rohingya-not-help-them

8   Fortify Rights. (2019). Tools of Genocide—National Verification Cards and the Denial of Citizenship of Rohingya Muslims in Myanmar. https://www.fortifyrights.org/downloads/Tools%20of%20Genocide%20-%20Fortify%20Rights%20-%20September-03-2019-EN.pdf

9   Ibid. Page 10.

10   UNHCR. (2018, July 6). Joint Bangladesh/UNHCR verification of Rohingya refugees gets underway.

https://www.unhcr.org/en-us/news/briefing/2018/7/5b-3f2794ae/joint-bangladeshunhcr-verification-rohingya-refugees-gets-underway.html

11   UNHCR. (2019). More than half a million Rohingya refugees receive identity documents, most for the first time. https://www.unhcr.org/news/briefing/2019/8/5d4d24cf4/half-million-rohingya-refugees-receive-identity-documents-first-time.html

12   In response to a draft of the global report, UNHCR told us that "protecting refugees' personal data is an essential part of refugee protection. The organization adopted, as early as 2014, a Policy on the Protection of Personal Data of Persons of Concern to UNHCR and appointed a Senior Data Protection Officer to support its implementation across its programmes globally".

13   Radio Free Asia. (2019, July 29). Bangladesh Gives Myanmar 25,000 Rohingya Names for Potential Repatriation.

https://www.rfa.org/english/news/myanmar/bangladesh-refugees-07292019172753.html

14   Capili, A. (2019). Arnel Capili on Twitter: https://twitter.com/arnelcapili/status/1155764445462716416

15   Radio Free Asia. (2019, July 29). Bangladesh Gives Myanmar 25,000 Rohingya Names for Potential Repatriation. https://www.rfa.org/english/news/myanmar/bangladesh-refugees-07292019172753.html

16   A tripartite voluntary repatriation agreement is an agreement between UNHCR, the country of origin and the country of asylum that outlines details for the voluntary return of migrants to their country of origin, including the rights of refugees upon return and guidance for repatriation and reintegration.

17   UNHCR. (2018). Bangladesh and UNHCR agree on voluntary returns framework for when refugees decide conditions are right. https://www.unhcr.org/en-us/news/press/2018/4/5ad061d54/bangladesh-unhcr-agree-voluntary-returns-framework-refugees-decide-conditions.html

18   UNHCR. Communicating with communities on registration. Guidance on registration and identity management. https://www.unhcr.org/registration-guidance/chapter4

19   Bhatia, A., Mahmud, A., Fuller, A., Shin, R., Rahman, A., Shatil, T., … Balsari, S. (2018, December). The Rohingya in Cox's Bazar. Health and Human Rights, 20(2), 105–122: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6293360

20   The Engine Room addressed perceived fraud through duplication in Biometrics in the Humanitarian Sector. (2018). https://www.theengineroom.org/wp-content/uploads/2018/05/Oxfam-Report-May2018.pdf

21   Jacobsen, Katja Lindskov. (2015, April 1). "Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees". Security Dialogue 46(2), 144–64. https://doi.org/10.1177/0967010614552545

22   UNHCR. (1951). The 1951 Refugee Convention. https://www.unhcr.org/en-us/1951-refugee-convention.html

23   UNHCR. (2018). Chapter 5.2 Registration as an Identity Management Process. Guidance on Registration and Identity Management. https://www.unhcr.org/registration-guidance/chapter5/registration

24   Ibid.

25   Al Jazeera. (2019, August 25). "Genocide Day": Thousands of Rohingya rally in Bangladesh camps. https://www.aljazeera.com/news/2019/08/day-thousands-rohingya-rally-bangladesh-camps-190825055618484.html

26   BNI Online. (2019, September 9). Abul Kalam and 7 Camps-in-Charge transferred from Rohingya refugee area. Burma News International. https://www.bnionline.net/en/news/abul-kalam-and-7-camps-charge-transferred-rohingya-refugee-area
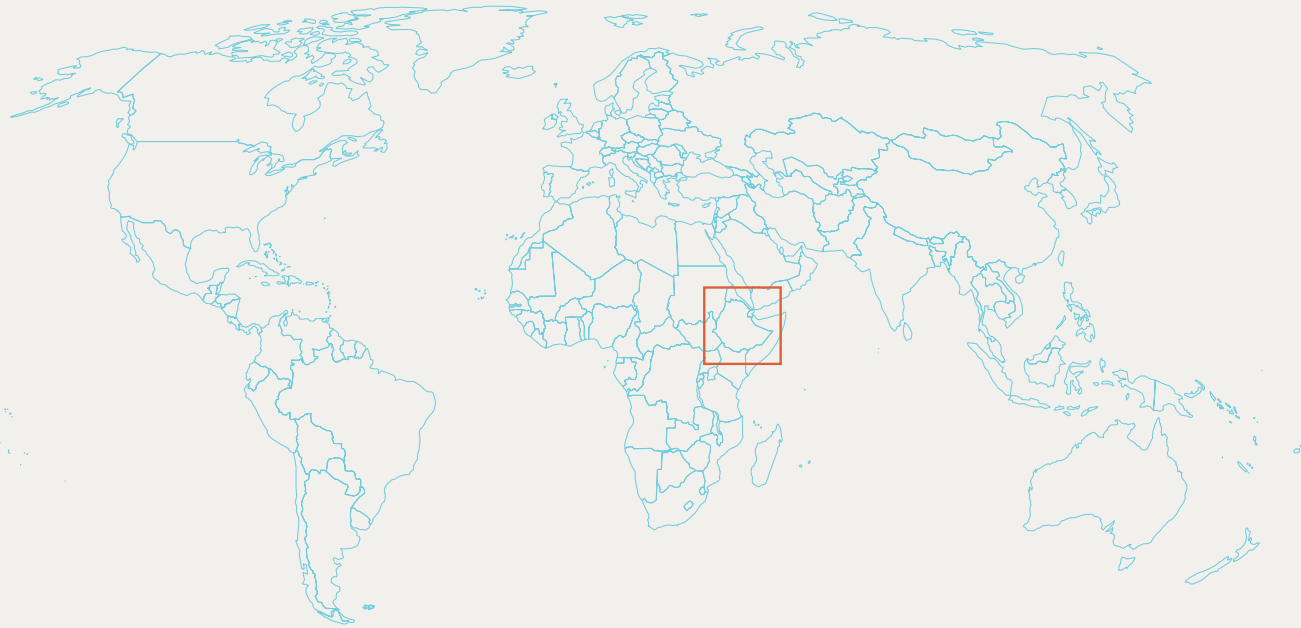
27   Anadolu Agency (2019, September 11). Bangladesh gets 'tougher' on Rohingya refugees. https://www.aa.com.tr/en/asia-pacific/bangladesh-gets-tougher-on-rohingya-refugees/1578938

28   BD News 24. (2019, September 3). BTRC orders telecom operators to stop services to Rohingyas in seven days. https://bdnews24.com/bangladesh/2019/09/02/btrc-orders-telecom-operators-to-stop-services-to-rohingyas-in-seven-days

29   Agence France-Presse. (2017, September 24). Bangladesh imposes mobile phone ban on Rohingya refugees. Yahoo News. https://www.yahoo.com/news/bangladesh-imposes-mobile-phone-ban-rohingya-refugees-073911274.html

30   Emont, J. (2019, September 3). Bangladesh cuts mobile access to Rohingya refugees. Wall Street Journal. https://www.wsj.com/articles/bangladesh-cuts-mobile-access-to-rohingya-refugees-11567541883

31   Rahman, Zara. (2015, December 22). Bangladesh will demand biometric data from all SIM card users. Global Voices. https://globalvoices.org/2015/12/22/bangladesh-will-demand-biometric-data-from-all-sim-card-users/

32   The Daily Star. (2019, September 02). All SIMs in Rohingya camps to be verified in 7 days. https://www.thedailystar.net/rohingya-crisis/no-mobile-phone-services-for-rohingya-refugees-1794367

33   New Age. (2019, September 11). No mobile internet in Rohingya camps. http://www.newagebd.net/article/84207/only-2g-services-in-rohingya-camps

34   Nahid, M. S. R. (2019, September 11). Mobile operators challenge Rohingya sim proof/ 'রোহিঙ্গা সিম' প্রমাণের চ্যালেঞ্জে মোবাইল অপারেটররা https://itdoctor24.com/2019/09/11/mobile-operators-challenge-rohingya-sim-proof

35   Agence France-Presse. (2017, September 24). Bangladesh imposes mobile phone ban on Rohingya refugees. Yahoo News. https://www.yahoo.com/news/bangladesh-imposes-mobile-phone-ban-rohingya-refugees-073911274.html

36   See, for example, Human Rights Watch. (2019, September 13). Bangladesh: Internet Blackout on Rohingya Refugees. https://www.hrw.org/news/2019/09/13/bangladesh-internet-blackout-rohingya-refugees# and Griffiths, J. (2019, June 25). Myanmar shuts down internet in conflict areas as UN expert warns of potential abuses. CNN. https://www.cnn.com/2019/06/25/asia/myanmar-internet-shutdown-intl-hnk/index.html

37   Note that in our case study on refugee camps in Ethiopia, UNHCR officials said that individuals who refuse the registration process do not receive aid.

Annex C

Digital ID in Ethiopian Refugee Camps:

A Case Study

Introduction

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

Our research in Ethiopia consisted of four in-depth interviews with key informants in UN-HCR and partner organisations as well as interviews and focus group discussions with 25 refugees in Histas and Jewi camps. This primary research was conducted between March and April 2019. All quotations from refugees and key informants come from in-person interviews and discussions during this period in Ethiopia. Additionally, while writing the research outputs (in November and December of 2019), we reached out to UNHCR's Division of Programme Support and Management for global report comments, which we have included here. More information on the methodology can be found in the global report.[1]

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.

Immigrants from South Sudan in Ethiopia

The Digital ID System

Ethiopia hosts more than 900,000[2] refugees from Eritrea, Somalia, Sudan, South Sudan and Yemen in 27 camps and 10 settlement areas across the country. In these camps, the United Nations High Commissioner for Refugees (UNHCR) carries out an ongoing registration process to enrol refugees in their digital ID system. Prior to this, Ethiopia's Agency for Refugee and Returnee Affairs (ARRA) was, according to a UNHCR informant, documenting refugee data in spreadsheets.

For biometric registration, comprehensive information – including educational and occupational history, the locations and names of family members, 10 fingerprints, iris scans and photographs – is gathered along with each person's camp residency (house number, block and zone). For children aged five and over, only fingerprints and a photograph are taken. The UNHCR Registration Official in Addis Ababa told us that approximately 500,000 had been registered at the time of our research in April 2019.

Aerial view of the Malkadiida refugee camp in Ethiopia

We were told that after registering, refugees receive a certificate with basic personal data, such as name, age and marital status, and those above 14 years old receive a physical ID card, which is valid for three years. The card itself does not hold any digital data (i.e., there is no digital chip in the card). As with UNHCR's registration services in all areas where they provide humanitarian assistance, one of the purposes of the digital ID system they oversee in Ethiopia is to provide refugees living in camps hosted by the nation with an identification card. UNHCR estimates that in the last decade more than 70,000 refugee children have been born in Ethiopia without birth certificates, and an additional 42,900 children are unaccompanied or separated from their families.[3] The registration process is also intended to address issues of protection for these children, ensuring that they have access to education and basic social services.

Additionally, biometric registration is commonly used in humanitarian contexts as an approach against 'double counting'[4] – that is, when the same person registers multiple times, which can complicate planning and logistics. In Ethiopia, however, a UNHCR informant told us that of more than 500,000 refugees registered for digital ID, fewer than 500 double registrations (less than 0.1%) have been found. This low figure indicates that double counting is not a significant problem in this population, although UNHCR may still be expected by donors to report exact numbers.

A key informant reported that UNHCR is in the process of creating a universal database that can be accessed by relevant UNHCR offices around the world. As described to us, their goal

is to make it possible for UNHCR staff to verify that someone who arrives in Greece, for example, was registered in Ethiopia prior to arrival. The consequences of this move to a centralised database could be significant for refugees concerned that they are treated differently depending on their country of origin.[5]

Additionally, a UNHCR informant reported that a memorandum of understanding between UNHCR and the Ethiopian government requires information gathered through this registration process to be shared directly with the Ethiopian government. Comments from UNHCR's registration officer based in Addis Ababa indicated that the existing agreement in place leaves no space for in-country staff to adjust what data is collected or how, based upon what they are seeing in real time.

Fortunately, in the new refugee law adopted by the Ethiopian government in 2019,[6] Article 44 addresses refugee data privacy, barring the disclosure of information to the authorities in refugees' country of origin.[7] This protection is critical because many of these refugees were forcibly displaced due to conflict in their home countries and could be targets of further persecution. Although Article 44 is not comprehensive, it is a critical first step in ensuring the safety of people who are threatened by their governments. Outside of the refugee law, Ethiopia has not passed data protection legislation that applies to the whole country, so it is not clear how they manage information about refugees that does not fall within the Refugee Proclamation.

Abuna Yem'ata Guh in Tigray, Ethiopia

Lived Experiences

The interviews and focus groups that were conducted in Ethiopia in March-April 2019 provide insight on the lived experiences of refugees interacting with this system. 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 refugees do not have one unified experience. Some of the experiences described in this case study may contradict official reports or UNHCR and ARRA guidelines.** We aim for these learnings to become part of the broader discussion on digital ID solutions in humanitarian contexts.

Awareness and understanding

Among refugees we spoke to, those going through biometric registration perceived the associated data collection as a necessary step towards accessing basic services, and, therefore, many appreciated receiving an identification card. For refugees who have been able to move out of camps, the ID card allows them to get a driving license and bank account, both of which are particularly helpful for those wishing to integrate into Ethiopian society and/or needing to provide for themselves and their families. UNHCR has guidance[8] on communicating with refugees communities about registration, and several interviewees reported that authorities made announcements block by block of the benefits of digital ID.

Others said they heard of the benefits from fellow refugees.

Many refugees we spoke to saw getting an ID card as a good development because it gives them access to the services, mobility and safety they lacked. Our research team noted the relief that people display upon receiving their cards but was careful to point out that refugees do not see any alternative to giving their personal data if they want to receive assistance.

Awareness of the need and use for biometric data is another story, however. Interviewees had very low levels of awareness about what the system itself was doing and what would be done with their data. We found that most people were aware of why their fingerprints are taken, but there was very little awareness of the purpose of iris scans. As one refugee said, "It is scary to ask these questions [about the purpose of iris scans]. I am scared to go into the offices and ask questions. I would've been happy if I was able to ask, but I am fearful".

When comprehensive biometric registration began, some refugees heard that if their irises were scanned and fingerprints taken, they would subsequently be unable to leave the country. One UNHCR staff interviewee noted that some people, especially refugees from Yemen, did not turn up for registration in the beginning and said this may have been due to iris scans. We were told that UNHCR made the decision to cut assistance to these individuals until they registered. This decision led to an increase in registration numbers.

Within the camps, misinformation amid a background of uncertainty appears to leave people fearful of what might happen to both their data and themselves. For example, there are (unsubstantiated) rumours of people disappearing from Histas Camp. While these rumours are not connected to biometrics, they give a sense of the uncertainty within the camp. Coupled with the lack of awareness about what biometric data is used for, uncertainty like this could easily lead to rumours of data being used against refugees. Misinformation and rumour-spreading within refugee camps is not a new problem, though the consequences could be severe.[9]

Lack of informed consent

Ensuring that people are informed about the purpose of the system and the consequences of gathering personal data is part of the informed consent process required by UNHCR policy,[10] but we came across very few examples of informed consent being obtained. Unfortunately, 24 of the 25 refugees interviewed in Histas Camp and Jewi Camp said they were not informed about what their data would be used for, and 15 of the 16 who had already completed biometric registration said they were not asked for consent before their biometric data was collected.

This failure to follow UNHCR's informed consent guidance was confirmed by an interviewee from a partner organisation who described a rushed process with photographs sometimes taken as people talked. Moreover, we witnessed registration processes where informed consent for biometric data was not obtained. Again, this failure goes against UNHCR policy, which likely indicates a need for better training or enforcement in the field, or at the very least, dedicated consideration of policy operationalisation that leaves refugees feeling respected and not fearful when it comes to their rights and biometric data.

People also said that they had been told explicitly that not giving fingerprints meant their assistance would be cut. Informed consent requires voluntariness and willingness, but these vital steps are missing when refugees view giving personal data as a necessary step towards accessing basic needs such as food and shelter. One refugee told us, "Of course they didn't ask for my consent", indicating that the lack of informed consent did not come as a surprise. Indicating that this power dynamic and lack of agency are nothing new, another noted, "As a refugee, we do not have much say. You do as you are told".

UNHCR and government staff we spoke to noted that they had not yet seen anyone refuse to provide fingerprints. This is largely unsurprising given that refusing to provide fingerprints is effectively understood as a rejection of assistance.

Registration barriers

Most people completed comprehensive biometric registration without incident, but several problem cases appeared in our interviews. For example, in one case a woman did not have proof of her divorce, which took place back in Eritrea: "I do not have an ID. I have to prove that I am not married and I am now struggling to get that proof. The children I had from my husband are being processed, but my other child and I have been unable. The fact that I haven't proved my divorce is holding back our process." UNHCR has since told us that this problem would not be a barrier to registration.

Some individuals were not in a fit condition to provide accurate answers upon their arrival in Ethiopia. One person described misunderstanding 'place of birth' as 'arrived from', which meant the system categorised them as being born in Ethiopia, instead of having arrived from a different part of Ethiopia. As a result of this data error, the system does not recognise this individual as a refugee from outside the country, leaving them unable to receive assistance, though UNHCR disputes this claim.

People we spoke to noted great difficulty in correcting small data entry errors, such as spelling mistakes and date of birth errors. These inconsistencies created issues further down the line, in some cases causing assistance to be halted.

A community mobiliser described reluctance among some Christian refugees to show up for comprehensive biometric registration because they believed their data would go to the Illuminati.[11] Community leaders were able to convince them that the Illuminati only seek wealthy people and would not be interested in people without money, and the Agency for Refugee and Returnees Affairs (ARRA), the Ethiopian government office that works with UNHCR, informed the group that they would not receive food if they did not register. Since then, more Christians have been registering.

Grievance reporting

We observed a litigation desk, where a lawyer is available to give information about problems or resolving errors. In addition, there were civil society representatives, notably from the Norwegian Refugee Council, providing support to people needing to alter their information. Small changes can happen then and there, but more significant changes (e.g., changing someone's age from 20 years old to 16 years old) must happen through court. In one camp, there was a 'mobile court' staffed by a judge who comes from the city to hear court cases on an on-demand basis together with people from the government.

Additionally, we observed that most of these help desks were run by men. Only one was run by a woman. This gender disparity creates a potentially intimidating environment for women seeking to report their problems and could act as a deterrent, especially given the cultural norms of many refugees living in Ethiopia.

If people refuse to give their fingerprints, they are sent to the litigation desk where someone further explains why their fingerprints are needed and discusses the refusal with them. Crucially, if the individual continues to refuse, they are told that this is being done under their own risk because, to quote a UNHCR informant, "they might risk losing assistance" as a direct consequence.

Civil society

A 2009 law severely restricted civil society in Ethiopia, but in 2019 the new government relaxed prohibitions.[12] While there are still some limitations, opportunities for civil society have opened up. Generally speaking, Ethiopian civil society is so far focusing on traditional human rights issues such as torture and forced disappearance. Similar to many other countries in the region, digital issues are not a priority.

Civil society has a unique opportunity in Ethiopia, however. Unlike in many host countries, refugees in Ethiopia are allowed to settle outside of camps. In January 2019, Ethiopia passed a law that gives almost one million refugees the right to work and live outside of camps (Bhalla, 2019),[13] a refugee integration step that has been hailed as one of the most progressive refugee policies in Africa.[14] This move can enable refugees to engage with civil society organisations addressing human rights.

As we observed both in person and through research, the Ethiopian government seems friendly towards refugees, which means that engaging with the government could be a viable advocacy strategy for civil society with enough resources. Civil society in Ethiopia may tread lightly as they determine exactly how supportive the new government is of both their work and refugee rights.

According to a UNHCR informant, the Ethiopian government is planning a national digital ID system based on BIMS, which makes the findings in this report even more vital for local civil society. Local populations can learn from refugee experiences with digital ID and advocate for better systems and appropriate protections.

Conclusions and Recom-mendations

Lack of understanding around various aspects of the registration process and failure to obtain informed consent were the most significant problems we found, and both feed into registration barriers and the limitations of grievance reporting. We encourage UNHCR to re-consider the conditions under which they gather biometric data from refugees – at the very least, providing strong checks for ensuring that their informed consent policy is followed in the field.[15] Critically, each person going through the registration process should understand what biometric data is being collected and how it will be used.

UNHCR's official policy on informed consent notwithstanding, the bigger issue is whether or not refugees are in a position to give meaningful, informed consent. The power asym-metry at play in humanitarian contexts means that people who are dependent on refugee agencies for basic services have extremely low expectations of how their rights should or could be respected. The lack of power these refugees experience and the rights violations that led them to rely on humanitarian assistance for basic needs are in some ways further

compounded by the way their data is gathered.

The refugees we interviewed did not feel able to assert their right to privacy or their right to know how their data is used. The most vulnerable people we spoke to noted that thinking about their data rights was of very little concern to them in the face of much more visible and pressing needs, such as shelter, access to water and physical safety. After listening to refugee stories, hearing them ask for help with more rations and discovering that visible groups nearby had not received food because they did not have IDs, it became clear to us that people who are hungry, or even starving, are not in a position to give informed consent.

The Engine Room is committed to further exploring fundamental problems with informed consent and to supporting civil society to establish more responsible processes for working with biometric data of vulnerable groups. We urge civil society, researchers, decision makers and developers of digital ID systems and processes to consider and push for alternatives

Abuna Yem'ata Guh in Tigray, Ethiopia

that take power dynamics into account and maintain the dignity and rights of refugees. This could happen in multiple ways, such as improving grievance reporting processes to identify priorities, developing meaningful alternative processes for those who might not feel comfortable providing biometric data and, internally, rethinking information management processes.

Finding ways to recognise the agency and dignity of refugees would, in the long-term, strengthen trust between those receiving assistance and humanitarian organisations, open up more possibilities for feedback loops that would strengthen programming and the provision of assistance, and ultimately meet core humanitarian goals of respecting dignity.

Finally, as civil society opportunities open up, we hope to see groups further incorporate refugee rights into their work and engage refugees directly on these issues to be sure their voices are heard and they play a role in developing solutions. In particular, encouraging the government to expand their commitment to refugee data protection can support secure, responsible data collection processes with the potential to increase opportunities for this population. This support might, in turn, help to protect the privacy of all Ethiopians as the government considers its national digital ID plans.

Notes

1   The Engine Room. (2020). Understanding the lived effects of digital ID: A multi-country report.

2   United Nations High Commissioner for Refugees. (2019). Ethiopia: Global Focus—2018 Year-end Report. http://reporting.unhcr.org/node/5738#_ga=2.265964234.418983153.1571232719-1703704718.1553874537

3   United Nations High Commissioner for Refugees. (2018). Comprehensive refugee response framework: The Ethiopia model. http://www.globalcrrf.org/wp-content/uploads/2018/12/UNHCR-CS-Ethiopia-screen.pdf

4   The Engine Room and Oxfam. (2018). Biometrics in the Humanitarian Sector. https://www.theengineroom.org/wp-content/uploads/2018/05/Oxfam-Report-May2018.pdf

5   See, for example, Court calls Canada's treatment of 'safe country refugees' unconstitutional, by Nicholas Keung (2019, March 22) in The Star. Available at: https://outline.com/AWgeJx

6   See Ethiopia: Proclamation No. 1110/2019, by Ethiopian National Authorities. Available at: https://www.refworld.org/docid/44e04ed14.html

7   Note that UNHCR follows a Policy on the Protection of Personal Data of Persons of Concern to UNHCR.

8   UNHCR. Communicating with communities on registration. Guidance on registration and identity management. https://www.unhcr.org/registration-guidance/chapter4/

9   For examples of the consequences of misinformation and rumours, see Refugees misdirected: How information, misinformation, and rumors shape refugees' access to fundamental rights, by Melissa Carlson et al in Virginia Journal of International Law (57(3). Available at: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4039&context=facpubs

10   United Nations High Commissioner for Refugees. (2018). Chapter 5.2 Registration as an Identity Management Process. Guidance on Registration and Identity Management. https://www.unhcr.org/registration-guidance/chapter5/registration

11   'Illuminati' refers to a conspiracy theory that a secret society rules world affairs.

12   Freedom House. (2019). Ethiopia: Civil Society Proclamation Advances Essential Freedoms. https://freedomhouse.org/article/ethiopia-civil-society-proclamation-advances-essential-freedoms

13   Bhalla, N. (2019). Ethiopia allows almost 1 million refugees to leave camps and work. Reuters. https://www.reuters.com/article/us-ethiopia-refugees-rights-idUSKCN1PB2QH

14   Kiunguyu, K. (2019). Ethiopia is pioneering refugee integration. This Is Africa. https://thisisafrica.me/politics-and-society/ethiopia-pioneering-refugee-integration/

15   UNHCR has inspected the success of biometrics in the field before. A report in Kenya shows staff are fully trained on Standard Operation Procedure and a communication plan was successful in raising awareness about processes and rights among refugees in one camp. See Joint Inspection of the Biometrics Identification System for Food Distribution in Kenya, by UNHCR and World Food Programme (2015). https://documents.wfp.org/stellent/groups/public/documents/reports/wfp277842.pdf

Annex D

Digital ID In Nigeria: A Case Study

Introduction

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

Our research in Nigeria consisted of six in-depth interviews with key informants in Abuja and online, as well as interviews and focus group discussions with a diverse group of citizens, including internally displaced persons, people with disabilities, people living in rural areas and affluent areas, and civil society organisations. This primary research was conducted between February and April 2019. All quotations from key informant interviews and focus group discussions come from the field research phase during this period. More information on the methodology can be found in the global report.[1]

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.

Voters at presidential election in Abuja, Nigeria

The Digital ID System

Currently, at least 13 federal agencies and several state agencies offer ID services in Nigeria. Each agency collects the same biometric information from individuals, overlapping efforts within government agencies at a high fiscal cost to the country. Although the Nigerian government aimed to integrate all of these systems as far back as 2014, progress has been slow. The initial roll-out of the card, often referred to as an 'eID', was marred by a partnership with MasterCard, which some criticised as a commercial venture that branded citizen data.[2] By October 2019 only 19% of Nigerians had registered for the national digital ID designed to replace the siloed ID systems.[3]

Aerial view of Third Mainland Bridge in Lagos, Nigeria

To reach more people, the National ID Management Commission (NIMC) of Nigeria has collaborated with the World Bank to develop an ecosystem model designed to increase coverage of this single national ID by leveraging the public and private sectors to become enrollment partners with NIMC. A World Bank informant stated:

> The idea is that when you go to register for a SIM card and you don't already have a national ID, at that same registration process, you would be registered for the national ID. Same thing with the bank. Same thing, for example, with any kind of social programs, even health programs.

The Nigerian government aims to use the NIMC ID to provide a wide range of services, including "social safety net, financial inclusion, digital payments, employee pensions, agricultural services, healthcare, education, skill development and employment, law enforcement, land reforms, elections and census".[4] Both adults and children will receive the ID. At registration centres, staff collect each person's demographic data, photographs and 10 fingerprints before giving out a "microprocessor chip-based general multi-purpose identity card"[5] to those aged 16 and older along with a national identification number (NIN).

Lived Experiences

The interviews and focus groups that were conducted in Nigeria in February-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. **Some of these experiences may contradict official reports, but it is critical to understand that all residents of Nigeria do not have one unified experience.** We aim for these learnings to become part of the broader discussion on digital ID solutions in national contexts.

Low levels of public awareness

People we spoke to in Nigeria reported a general lack of awareness around the functions of the national ID, why so much data is collected and how data is stored. Our research showed that enrolment for the NIMC digital ID program is low because most people do not know the purpose of the card. Often, those who have registered did so simply because they could not access some service without a NIN or because they saw people queuing and, in the case of low-income individuals and especially those in internally displaced persons camps, hoped to receive some benefit such as food or compensation.

Furthermore, some interviewees claimed that the government wants people to enrol more quickly and is threatening to withhold other key documents to make it happen. "We were threatened that if you don't have a national ID card, you won't be able to renew your international passport, that's why we went to register" said one interviewee. We were told that this harassment encouraged some Nigerians to go ahead and complete the registration process.

Little to no public consultation

The World Bank's digital ID development and implementation plan with the Nigerian government describes the importance of public engagement, including a stakeholder engagement plan with special attention to state governments, "regular communication with the general population" and "formal consultations with vulnerable groups".[6] While some interviewees mentioned hearing about the new ID on television and the radio, most of the interviews and focus groups demonstrated no knowledge of any public consultation.

One focus group of people with disabilities had heard about a World Bank meeting (and the World Bank confirmed that they did consult people with disabilities) but did not know anyone who was present. The leader of this group stated, "If our voices were heard and we were seated at the table, maybe the content and the process won't be so faulty. There's no sense of ownership". Without buy-in, people feel no reason to register, and even those who do register do not see much value in the ID. This lack of "ownership" is a fundamental problem for a government agency aiming to register approximately 200 million people. In fact, more than 700,000 people who have registered have not even picked up their card.[7] This experience also speaks to the need to raise public awareness about the consultations that occurred. People may still have feedback if they see that their needs are not fully addressed, but they will be more confident in the system knowing that decision makers reached out to their broader community and will be more likely to have faith that their complaints will be heard.

Barriers to registration and use

In Nigeria registration barriers most affect people with low income, people from rural communities and people with disabilities. Everyone we spoke to said the registration process is extremely long. Whereas wealthier people can afford to pay for for registration officers to come to them or pay to, as interviewees said, "jump the queue" even though these bribes are supposedly not allowed, people with limited resources stand in registration centre queues for anywhere from hours to days. One key informant described the process as "very, very difficult. It's long and the centres are extremely busy. People are queuing for several days".

Queuing all day at registration centres is even more complicated for people who have to travel longer distances to reach centres. Travel costs money and may mean missed work. Additionally, the registration process hinders participation from people in rural communities whose religion dictates conservative gender norms. Despite the government's goals of financial inclusion and aid distribution, our research shows that these IDs have not reached many people in rural areas in need of aid.

Many of the registration locations are not accessible to people with disabilities. A blind man said he was given a form to fill out and had to ask another person waiting to register to fill it out for him. A disabled woman spoke of waiting in line to collect her card with no place to sit. After more than an hour, her legs were failing her and she asked for help, but no one responded due to the noise of people in the room. She had to yell to get the attention of the registration staff. Another participant in a focus group for people with disabilities reported similar experiences: "[Wheelchair] riders will tell you 'from the gate we got discouraged and turned back', the deaf will tell you that 'some officials will just give you attitude; they are just not patient enough to understand'". This person then shared what he would do if he were in charge:

We are the poorest of the poorest, so I would not want people to come five times simply

Additionally, there is confusion around the recognition of disability. Registration forms ask people if they have disabilities but do not enable them to specify the type. The card itself does not include any information on disability, which caused disabled people we interviewed to be concerned about misunderstandings. A deaf person, for example, expressed concern that the card did not inform people of this disability. He was almost arrested at a military checkpoint, where soldiers suspected him of being a Boko Haram member because he was unable to respond to their questions. His ID, which did not communicate his disability, was useless in this instance. What saved him was the sudden appearance of someone who recognised him. It is not clear why information about disability is collected and how it is used if it is not then displayed on the card itself or when scanned.

Finally, we spoke to several people who still had not received their IDs after several months, and even years, of waiting. A woman who was displaced due to the Boko Haram insurgency registered in 2016 and only had a paper document to show for it; she was still waiting for her plastic ID. Another forcibly displaced person told us each time he went to retrieve his card the computer was not functioning properly or the monitor was down. Eventually, he lost his SIM card, leaving the government no way to let him know his card is ready.

Several months after our field research phase ended, NIMC announced on Twitter in October 2019 that there would be a fee of NGN 3000[8] per person to renew the national digital ID.[9] This development was met with ire and frustration, especially from people who have waited years and still have not received their ID card.[10] Our research shows the many ways

this system has already excluded people, and this fee will only compound that problem and exacerbate existing inequalities.

Lack of informed consent

People we interviewed in Nigeria said there is never any mention of an informed consent process. Simply showing up at a registration centre is seen as giving consent. In fact, the widespread assumption of presence equalling consent led at least one interviewee to refer to the researcher's explanation of informed consent as "demanding for special consent" – the very premise of 'informed consent' was seen by participants as extraordinary and funny because consent is not usually collected. This view was so widely held that there was rarely further discussion.

This finding is in sharp contrast to best practices around data collection. Obtaining informed consent is widely regarded as a necessary step in identification systems in order for people's rights to be respected, and it must involve actually asking the person registering for their permission before collecting data, especially biometric data. Furthermore, lack of informed consent can be linked to the lack of "a sense of ownership" described above. When processes designed for digital ID systems fail to respect people's rights and to enable them to make decisions about their data, it harms the relationship of trust between people and governing institution and prevents shared ownership.

Data protection

Nigeria's new digital ID system will be used across several government agencies as well as many private sector companies. Key informants told us there is already a high rate of non-consensual data sharing, including the selling of data sets between government agen-

cies and financial institutions, telecommunications companies, and third-party marketers. One interviewee stated, "Yes, banks have access to my information… and Nigeria Ports Authority have access to our information".

Many focus group participants believe that their data is not safe with the government and private sector, but they hand it over anyway due to lack of choice. The high rate of cybercrime in Nigeria has many convinced that people working in banks give thieves access to their data. A focus group participant stated, "I think that there is a fear that this information could be shared because the issue of cyber crime in Nigeria could not have been successful if not in collaboration with the in house [staff]".

Still, members of civil society told us that data protection is generally not considered much of an issue by the public. Due to the high rate of poverty in the country, the average citizen is not concerned about what the government wants to do with their data. They are more worried about surviving and providing for their families, and privacy is seen by many as a luxury concern. As a key informant said, "[The government is] collecting [data] because nobody is complaining about the protection law."

Focus groups with internally displaced persons revealed a combination of gratitude for the assistance and opportunities available through digital IDs and concern about privacy and the purpose of data collection by the government and the World Food Programme. One woman said, "I don't really know what it is being used for. Sometimes I am afraid that maybe my name and pictures are being used for diabolical reasons, but I always pray to God for safety." Repeated photographs (likely for purposes other than digital ID) were a serious concern. Two others in the same focus group complained about people taking their photographs daily but never following through on promises:

> The pictures they snap are always too much, and they will always say that after taking the

These experiences with data collection, especially with photographs, by powerful institutions like the Nigerian government and the World Food Programme, seem to have increased individual attention to data, especially among particularly vulnerable populations.

Fortunately, Nigeria's National Information Technology Development Agency adopted the Nigeria Data Protection Regulation[11] in January 2019. As we have seen with new data protection legislation in other parts of the world,[12] this regulation incorporates some components of the European Union's General Data Protection Regulation.[13] In a country with significant digital security problems where data is commonly shared without consent,[14] success will depend on education and enforcement.

Civil society

The lack of public interest, and therefore, public pressure, makes advocacy in the digital ID space difficult. Nigerian civil society is fairly small and poorly funded, and it is difficult for organisations to take on new issues when those they already address are major problems people struggle with on a daily basis, such as poverty. In a focus group discussion with civil society representatives, one participant summed up the problem:

I feel that we should be more engaged on those issues, but the reality is that we are not part of it simply due to capacity and resources. For me, it's not only about not wanting to be all things to all men; we simply don't have the capacity to be all things to all men.

These challenges leave digital rights organisations to carry the burden of pushing for change from a powerful government. Paradigm Initiative, a digital rights organisation, has been engaged on the issue of digital ID going as far back as the Mastercard partnership with the government. A civil society interviewee reported:

> [C]ivil society organisations in themselves are too small to take on government individually, and even though Paradigm Initiative has taken that battle, you've not seen the entire CSO sector rally in support so as to make a bit more impact. So you have one small organization with tiny resources fighting this Goliath. The best you can do is just throw up some issues. They can bury you in court — they have all the resources – if they really don't want to provide that information.

Still, Paradigm Initiative was able to raise awareness about the risks of a foreign corporation having access to the NIMC database and has since pushed for the Digital Rights and Freedom Bill,[15] which remains unsigned.[16]

Conclusions and Recommendations

Given the overburdened state of civil society in Nigeria, it would be good to see regional and international organisations, advocates and funders invest resources into a wide range of civil society organisations in the country. Supporting civil society in understanding how digital ID intersects with their issue areas and why it is important for the people they serve can make a difference, but these groups also need the financial and team capacity to incorporate digital ID concerns into their work. This support can create a network of activists and organisations taking on issues such as consent and data protection with Paradigm Initiative leading the way, thereby strengthening work that has already started and increasing pressure on the government in a way a single organisation cannot accomplish.

The most vital issues we found in Nigeria revolve around access and information. The Nigerian government's aim of financial inclusion cannot be met when many of the very communities they seek to include face barriers to registration. Advocacy strategies could reflect the needs of the wide range of communities served by civil society from people living in poverty

to people with disabilities. Tackling the renewal fee and costs associated with registration will be paramount for the large number of Nigerians with few financial resources. Registration centres that are accessible for people with disabilities and people living in rural communities, especially women who, for cultural reasons, may not feel comfortable waiting next to men, are critical to reaching the most marginalised populations.

Finally, Paradigm Initiative's work on the Digital Rights and Freedom Bill is paramount. Any investment in digital ID improvements should prioritise advocating for data protection and ensuring the rights of Nigerians.

Notes

1   See The Engine Room. (2020). Understanding the lived effects of digital ID: A multi-country report.

2   See, for example, Branding Nigeria: MasterCard-backed I.D. is also a debit card and a passport, by Alex Court (2014, September 25), CNN. Available at: http://edition.cnn.com/2014/09/25/business/branding-nigeria-master-card-backed-i-d-/index.html. And Nigeria's Orwellian biometric ID is brought to you by MasterCard, by Siobhan O'Grady (2014, September 3), Foreign Policy. Available at: https://foreignpolicy.com/2014/09/03/nigerias-orwellian-biometric-id-is-brought-to-you-by-mastercard/

3   Sanni, K. (2019, OCtober 20). National ID card is free, but only 19% Nigerians are registered. Premium Times. https://allafrica.com/stories/201910210021.html

4   National ID Management Commission. (2017 June). A strategic roadmap for developing digital identification in Nigeria. https://www.nimc.gov.ng/docs/reports/strategicRoadmapDigitalID_Nigeria_May2018.pdf

5   The World Bank. (2016). ID4D - Country diagnostic: Nigeria. http://documents.worldbank.org/curated/en/136541489666581589/pdf/113567-REPL-Nigeria-ID4D-Diagnostics-Web.pdf

6   The World Bank. (2018). Project information document/integrated safeguards data sheet (PID/ISDS)—Nigeria digital identification for development project (p. 9). http://documents.worldbank.org/curated/en/501321536599368311/pdf/Concept-Project-Information-Document-Integrated-Safeguards-Data-Sheet-Nigeria-Digital-Identification-for-Development-Project-P167183.pdf

7   Sanni, K. (2019, October 20). National ID card is free, but only 19% Nigerians are registered. Premium Times. https://allafrica.com/stories/201910210021.html

8   At the time of writing (November 2019), this amount was equal to EUR 7.50.

9   Channels Television. (2019, October 15). Nigerians fume as NIMC attaches N3,000 charges to national ID renewal. https://www.channelstv.com/2019/10/15/nigerians-fume-as-nimc-attaches-n3000-charges-to-national-id-renewal/

10   Sahara Reporters. (2019, October 15). Backlash Greets NIMC Announcement Of N5000 For National ID Renewal http://saharareporters.com/2019/10/15/backlash-greets-nimc-announcement-n5000-national-id-renewal

11   National Information Technology Development Agency. (2019). Nigeria data protection regulation. https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf

12   For example, our Thailand case study notes GDPR-inspired legislation.

13   https://digitalguardian.com/blog/breaking-down-nigeria-data-protection-regulation

14   PUNCH. (2019, September 22). Concerns as Nigerian firms move to adopt data protection regulation https://punchng.com/concerns-as-nigerian-firms-move-to-adopt-data-protection-regulation/

15   Adegoke, A., & Ilori, T. (2019, August 3). Digital Rights and Freedom Bill Archives: The Leap and the Hurdles. Paradigm http://paradigmhq.org/tag/digital-rights-and-freedom-bill/

16   Ekwealor, V. (2019, March 27). Nigeria's president refused to sign its digital rights bill, what happens now? Techpoint.Africa. https://techpoint.africa/2019/03/27/nigerian-president-declines-digital-rights-bill-assent/

Annex E

Digital ID In Zimbabwe: A Case Study

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]

Aerial view of downtown city centre in Harare, Zimbabwe

With the country's plans for a national digital ID system tied to national security still under-way, 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 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 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 under-standing 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.

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 implemen-

tation 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 cer-

tain 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:

> 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 be-

tween 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.

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 Recom— mendations

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

Notes

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/

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

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

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

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

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

Annex F

Digital ID In Thailand: A Case Study

Introduction

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

Our research in Thailand consisted of six focus groups with different communities, six interviews with civil society organisations (CSOs) working with marginalised communities, and six interviews with government officials and IT experts. Additionally, our research team in Thailand hired local interpreters to communicate in migrant languages such as Burmese. This primary research was carried out between February and March 2019. All quotations from key informant interviews and focus group discussions come from the field research phase during this period. More information on the methodology can be found in the global report.[1]

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 that are not designed to address diversity of experience and identity.

The Digital ID Systems

Thailand's first attempt at a biometric digital ID system in 2005 was riddled with problems. The government expected to register 64 million people in three years without conducting a pilot or feasibility study, relied on technologies that were incompatible with one another, failed to provide clarity on how the card functioned and faced bureaucratic complications and accusations of corruption.[2] More recently, the development and piloting of a National Digital ID (NDID) platform to facilitate online transactions has begun,[3] though its roll-out has been delayed numerous times. In September 2018 the government approved a draft bill to set regulations for authentication and require the formation of a national digital ID company to build a platform and database.[4] Reports show a pilot phase starting with bank staff in January 2019,[5] but as late as October government agencies were apparently unable to exchange data as planned.[6] A proposed Government Data Exchange Center will not be fully complete for two more years. As of the time of writing (November 2019) there have been no more updates in projected timelines.

In the meantime, Thailand has a fragmented identification system, with multiple ID systems for different populations administered by five government departments at various levels of digitisation. As Thailand's digital agenda – and with it the widespread use of biometrics across different sectors – gains momentum, it is important to step back and consider the identity experiences of different groups. Since the country's three to five million migrant

workers are particularly marginalised and face a complex identification process,[7] much of our research focused on this population.

While we explored how the proposed upcoming national ID system – which will unite some of the discrete systems – is being rolled out, we also documented people's experiences with the Thai government's identification sector more generally. Firstly, we examined the national ID system reserved for those over 60 years old, which focuses on delivering welfare benefits, such as income and healthcare. Secondly, we focused much of our attention on the ID system used by migrant workers to enable legal employment, known as the 'pink card'. Thirdly, we spoke to other marginalised communities about the impact the country's various digital ID systems have had on them.

Under the 'pink card' system, migrants from Laos, Cambodia and Myanmar who enter Thailand without appropriate Thai documents must register for an ID known as the 'pink card',[8] used by government agencies, banks and other service providers to verify identity. It is not clear whether or not this ID is attached to biometric data, but a government informant did tell us that the Thai government collects the DNA of a certain number of migrants each year for "security purposes". Information gathered for this ID includes name and surname, date of birth, current address in Thailand, date of validation, name of employer and address, and type and place of medical care. Migrants register through an employer and are required to re-register with a new employer each time they change jobs.

This NDID system, on the other hand, is primarily focused on banking and financial services and is intended to "enhance digital security to facilitate online transactions, and enable greater access to bank accounts and lending… based on facial recognition and blockchain-powered identity authentication technology".[9] Reports have highlighted interoperability with "UN digital ID and e-authentication collaborations in the Association of Southeast Asian Nations", suggesting potential for data sharing.[10] The development of this system is part of a growing

trend towards the use of biometrics in Thailand, including mandatory checks to authorise SIM card purchases,[11] and the reported requirement of mobile phone users in three majority-Muslim states to submit photos for biometric facial recognition, a move criticised by local advocacy groups[12].

Technology and legal experts have expressed concerns that the NDID system will be no more useful than the previous system, will fall prey to authentication failures and privacy violations, and will be weakened by lack of faith in government reliability.[13] Some Buddhists have also spoken out against digital ID as incompatible with Buddhist dogma.[14] A key informant from the National Economic and Social Development Council countered these concerns by informing us that the government obtained all necessary information for planning and implementation.

Lived Experiences

The interviews and focus groups that were conducted in Thailand in February-March 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. **Some of these experiences may contradict official reports, but it is critical to understand that all residents of Thailand do not have one unified experience.** We aim for these learnings to become part of the broader discussion on digital identification solutions in national contexts.

Little public consultation

The Thai government seems aware of the need for at least some public consultation on their upcoming national digital ID system. They scheduled a public hearing in July 2018 prior to the passage of their digital ID law,[15] and the Ministry of Digital Economy and Society opened public consultation on the Personal Data Protection Bill for two weeks in September of 2018.[16] Still, these opportunities are not accessible for many of the most marginalised populations in Thailand, and we found no evidence of intentional consultation with these communities.

Similarly, neither the pink card nor the ID for people over the age of 60 show much evidence

of public consultation. Migrants we spoke with noted that the pink card system was an ongoing source of frustration and confusion, demonstrating a lack of effective consultation in the system's design. The people we interviewed about the ID for people over age 60 had a number of ideas and concerns they wanted to share with the government, including that some of the government schemes related to the ID are unreasonable for this population, but they did not feel they had opportunities to share this feedback.

Registration barriers

As of February 2019, there were more than three million documented (and likely many more undocumented) migrant workers in Thailand,[17] the vast majority of whom came from Myanmar. Migrant workers are required by law to register with the Thai government through their employers in order to receive work permits and identification documents. This population must re-register each time they change jobs, which happens frequently due to the precarious nature of migrant work. Information is typically not available in native languages, and labourers must provide a range of documents to support the application process.

In addition to a helpline, the Ministry of Labour has a website[18] where migrant workers can ask questions, and it provides in-person support in some provinces. However, this support isn't delivered consistently and can be hard to come by. Although some provinces have an official to support migrant labourers, one interviewee described how migrants who encounter problems struggle to get support from officials: "If we don't understand new rules, we used to call the hotline of Ministry of Labour, but no one picks up the phone or our calls have been transferred to several officials without any answer or any help." Even when officials do answer calls, this person told us, they do not seem to care or to be informed about migrants' ID needs.

Lack of information and accessibility around this process have led to a dependence on private,

unregulated brokers for information and support in navigating these complex bureaucratic procedures.[19] These brokers are also an important stakeholder for ethnic minorities in Thailand who have not been granted full citizenship. While some brokers facilitate the livelihood of migrants and ethnic minorities, these groups are particularly vulnerable to exploitation.[20][21] As one interviewee said, "It is so hard to refuse the service of head-hunters or paying for shortcut ways because we don't know the Thai system and understand Thai language and we can't wait so long to get our paper done." This echoes challenges encountered in other digital ID systems, where the 'analogue' components of a system, including community engagement and information provisions, are forgotten or deprioritised, resulting in exclusion and loss of trust.[22]

Civil society organisations play an important intermediary role for marginalised groups in Thailand, helping them access ID cards and navigate registration processes through troubleshooting, advice and easy-to-understand resources in migrants' native languages. In some cases, they collect data from people and complete registration on their behalf. Although this tactic is effective in increasing access and creating opportunities for CSOs to advocate for migrant needs and rights, it raises concerns around data protection and privacy. When CSOs are acting as intermediaries in an ad-hoc way, it is impossible to guarantee the security and privacy of data that is collected. Furthermore, an organisation helping migrants told us that the brokers migrants often rely on "cause confusion" and make false claims about the work of civil society that have organisation staff fearing for their safety.

Rights restrictions

Regardless of which digital ID systems people were subjected to, those who found themselves pushed furthest into the fringes of society expressed deep frustration and concern. Women's and indigenous rights groups interviewed as part of this work raised concerns around the use of digital ID systems in the surveillance and suppression of marginalised

communities. One advocacy organisation spoke of trafficking survivors they supported being "blacklisted" by financial institutions – unable to get loans or passport extensions – because of data reflecting experience with sex work: "We are pleased that this woman was helped but later on she shared her problem with us that she can't apply for her new passport or any loan because her record is under the blacklist."

In a focus group with indigenous people, participants expressed a lack of understanding about why their data was collected, as well as how it was used and shared between government departments:

> It is convenient for government officials to access individual information through our ID card. Our individual information has been shared with every government agency. We don't have a clue how each agency uses our data. We don't have access to our own information and update it.

Digital ID systems were seen as a way for the government to track and control the community. One interviewee stated:

> Government officials know where we live and suggest us not to go outside of our village to join political protests. At one point, government officials knew that our leaders went out of village and organised a consultation with other villagers without informing our leaders.

While this link between digital ID and government surveillance of indigenous people is unsubstantiated, the views of these communities and their advocates reveal a lack of trust in both the government and digital ID systems.

Conclusions and Recommendations

In this work, we examined the national ID system along with systems affecting two specific communities whose rights are often denied: migrant workers and elderly people. The issues we observed with the migrant workers' pink card in particular raise serious concerns about how the design of ID systems can limit access through language barriers and lack of support around information and navigating registration. That said, the pink card did indeed grant benefits to people who were able to obtain the card, demonstrating the positive potential of these systems.

One of the biggest lessons from the research in Thailand is that the reliance on fragmented infrastructures makes it difficult for both affected populations and potential advocates to properly understand the systems they interact with, which leads to confusion and a decreased ability to push for change. Although NDID may reduce the need for multiple IDs, this system raises questions around data sharing across government agencies and various private sector partners. As we saw with the sex worker example above, broad data sharing

can have an adverse impact on already vulnerable populations.

Moreover, the experiences shared with us, especially around the pink card, highlight issues that will undoubtedly be raised in other ID systems. Migrants and non-citizens are often the first to face a denial of rights, which makes these experiences important warnings for institutions implementing digital ID and civil society advocating for the needs of such populations. Addressing the problems found in this research can go a long way toward building user trust and ensuring full enjoyment of the benefits of digital ID systems. If the Thai government aims to make implementation of the NDID far more effective than the platform developed in 2005, regular engagement with diverse constituencies will be critical.

Thailand has a number of digital rights organisations, such as Thai Netizen and Manushya Foundation, both of which advocated for changes to the Cybersecurity Act in late 2019[23] and are well versed in some of the issues surrounding digital ID. In fact, strategic litigation and legal advocacy may play a valuable role in changing the national digital ID system, thanks to the Personal Data Protection Act[24] based on the European Union's General Data Protection Regulation and passed by the Thai government in early 2019. The presence and, hopefully, enforcement of this data protection regulation offers potential for civil society looking for strategies to support a more rights-based approach to digital ID in the future.

Notes

1   See The Engine Room. (2020). Understanding the lived effects of digital ID: A multi-country report.

2   Gunawong, P., & Gao, P. (2010). Understanding eGovernment Failure: An Actor-Network Analysis of Thailand's Smart ID Card Project. PACIS 2010 Proceedings. 17. https://aisel.aisnet.org/pacis2010/17

3   National Digital ID Platform (2019). https://ndidplatform.github.io/docs/introduction

4   Pornwasin, A. (2018, September 16). Mixed reactions to Digital ID draft law. The Nation Thailand. https://www.nation-thailand.com/national/30354611

5   Burt. C. (2019a, January 2). Thailand's decentralized national digital ID goes to testing ahead of mid-year launch. Biometric Update. https://www.biometricupdate.com/201901/thailands-decentralized-national-digital-id-goes-to-testing-ahead-of-mid-year-launch

6   Prachachat. (2019, October 6). ลุย "รัฐบาล 4.0" เร่งเชื่อมข้อมูลต้นดิจิทัลไอดี. https://www.prachachat.net/ict/news-378280

7   Blomberg, M., & Wongsamuth, N. (2019, August 30). New rules, new debts: Slavery fears rise for migrant workers in Thailand. Reuters. https://www.reuters.com/article/us-thailand-migrants-slavery/new-rules-new-debts-slavery-fears-rise-for-migrant-workers-in-thailand-idUSKCN1VK006

8   Isaan Lawyers. (2018). Pink ID Card for Foreigners in Thailand. http://www.isaanlawyers.com/pink-id-card-for-foreigners-in-thailand/

9   Burt, C. (2019a, January 2). Thailand's decentralized national digital ID goes to testing ahead of mid-year launch. Biometric Update. https://www.biometricupdate.com/201901/thailands-decentralized-national-digital-id-goes-to-testing-ahead-of-mid-year-launch

10   Bangkok Post. (2019, June 29). Digital ID scheduled for year-end. https://www.bangkokpost.com/business/1703996/digital-id-scheduled-for-year-end

11   Lee, J. (2017, February 2). Thailand government introduces fingerprint ID for SIM card registration. Biometric Update. https://www.biometricupdate.com/201702/thailand-government-introduces-fingerprint-id-for-sim-card-registration

12   Burt, C. (2019b, June 27). Thailand orders facial biometrics collection for SIM use in Muslim-majority states. Biometric Update. https://www.biometricupdate.com/201906/thailand-orders-facial-biometrics-collection-for-sim-use-in-muslim-majority-states

13   Pornwasin, A. (2018, September 16). Mixed reactions to Digital ID draft law. The Nation Thailand. https://www.nation-thailand.com/national/30354611

14   Kitiyadisai, K. (2004). Smart ID Card in Thailand from a Buddhist Perspective. Manusya: Journal of Humanities, 7(4), 37–45. https://doi.org/10.1163/26659077-00704003

15   Bangkok Post. (2019, June 29). Digital ID scheduled for year-end. https://www.bangkokpost.com/business/1703996/digital-id-scheduled-for-year-end

16   Yatim, S. (2018, October 24). Thailand 4.0: Digital ID, Cybersecurity, and Personal Data Protection Developments. Access Partnership. https://www.accesspartnership.com/thailand-4-0-digital-id-cybersecurity-and-personal-data-protection-developments/

17   International Labour Organization. (2019). TRIANGLE in ASEAN Quarterly Briefing Note. https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/documents/genericdocument/wcms_614383.pdf

18   Thailand Department of Employment. (2016). Complaint System for foreign Workers. https://www.doe.go.th/helpme

19   Human Rights in ASEAN. (2014, February 24). Myanmar Migrant Workers in Thailand Face Visa Extension and Passport Issuance Chaos and Extortion. https://www.humanrightsinasean.info/campaign/myanmar-migrant-workers-thailand-face-visa-extension-and-passport-issuance-chaos-and

20   Pollock, J. (2007). Chapter—Thailand. In Global Alliance Against Trafficking in Women (GAATW) (Ed.), Collateral damage: The impact of anti-trafficking measures on human rights around the world (pp. 171–202). Bangkok: GAATW. https://www.iom.int/jahia/webdav/shared/shared/mainsite/microsites/IDM/workshops/ensuring_protection_070909/collateral_damage_gaatw_2007.pdf

21   Asean Trade Union Council. (2017, March 3). Thai pink card workers ripped off by brokers. http://aseantuc.org/2017/03/thai-pink-card-workers-ripped-off-by-brokers/

22   Misra, P. (2019). Lessons from Aadhaar: Analog aspects of digital governance shouldn't be overlooked (p. 34). Pathways for Prosperity Commission. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-02/lessons-from-aadhaar20feb19_final.pdf

23   Zsombor, P. (2019, September 24). Rights Groups Urge Thai Government to Curb Powers in New Cybersecurity Act. Voice of America. https://www.voanews.com/east-asia-pacific/rights-groups-urge-thai-government-curb-powers-new-cybersecurity-act

24   Thailand National Authorities. (2015). Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act. Translated by Thai Netizen Network. https://thainetizen.org/wp-content/uploads/2015/01/personal-data-protection-bill-20150106-en.pdf

Image Credits

THE ENGINE ROOM

www.theengineroom.org