

8593
4-75924-384866-69
49-879505-6874748-9
3-688694995-684
64268-06837-0
702-356222-6
125689

A DIGITAL ID HANDBOOK

Strategies for Navigating Electronic Identification Systems



A DIGITAL ID HANDBOOK

**Strategies for Navigating Electronic
Identification Systems**

A People's Guide To Tech
In collaboration with The Engine Room

A Digital ID Handbook:
Strategies for Navigating Electronic Identification Systems
Published by A People's Guide to Tech, 2022

This work is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/4.0> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, CA 94041, USA

ISBN 979-8-9866082-0-4

Written by Mimi Qnuqha and Mother Cyborg (Diana Nucera)

Edited by Morgan Mann Willis and Corin Faife

Cover illustration and book design by Sylver Sterling

Research support from The Engine Room

Original research reports by ELSAM (Indonesia), Policy (Uganda), Stacey-Ann Wilson (Jamaica) and Amna Khan (Pakistan)

Printed and bound in United States of America

A People's Guide to Tech
Detroit, Michigan
www.peoplesguidetotech.org



Contents

- 6 A Note from the Authors
10 Glossary

15 A Brief Introduction To Digital ID

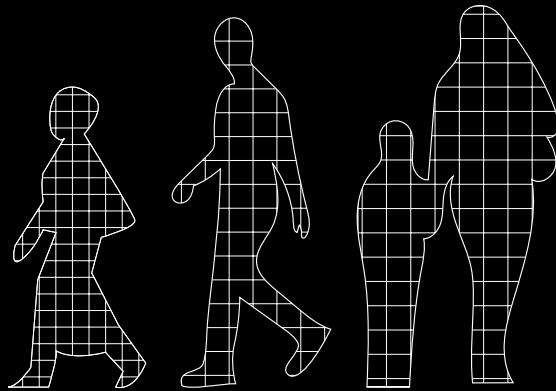
- 16 What Is Digital Identification?
23 Activity 1: From Identity to Identification
26 Why Digital Identification Systems?
32 Activity 2: Where Digital ID Meets You

35 Case Studies: Effects of Digital ID in Communities

- 36 Case Studies: Effects of Digital ID in Communities
40 Activity 3: Digital ID Systems Around the World
44 Living with Digital ID

59 The People's Power: Strategies for Navigating Digital ID Systems

- 60 The People's Power: Strategies for Navigating Digital ID Systems



A Note from the Authors

Across the globe, more and more countries are rolling out digital identification systems. These systems combine governmental desires to verify and track citizens with the capabilities of electronic technologies. Though they differ in their specifics, most share the same end goal: the creation of a single digital identifier to store each resident's personal data.

In 2020 and 2021, the Engine Room—an international organization that helps social justice groups use technology and data in strategic and responsible ways—published two reports detailing what it means to live with and organize around digital ID systems. The reports showed a troubling reality: organizers, civil society organizations (CSOs), and ordinary people were found to be among the last to learn about digital ID systems. Community responses to these new systems were developed as the digital ID systems were already being implemented.

This guide is meant to ensure that we are no longer caught off guard by the implementation of digital identification systems. It is a collaboration between The Engine Room and A People's Guide to Tech (APGT). At APGT, we make approachable materials that support organizing around technology. We've used The Engine Room's reports *Understanding the Lived Effects of Digital ID* and *Digital IDs Rooted in Justice* to create this handbook for anyone tackling issues arising from digital ID systems in their own country or region. We've designed this handbook especially for those who are encountering digital ID systems for the first time, but we've filled it with information and activities that can support even the most seasoned expert on electronic identification. Wherever you are located, the goal of this workbook is to make it easy for you to understand digital ID systems and create your own strategies to navigate them.

There are three parts to this guide. The first section, "A Brief Introduction to Digital ID Systems," provides context on what digital ID systems are so that you can develop a clear understanding of why they exist and how they work. The second section, "Case Studies: Effects of Digital ID in Communities" offers examples from research conducted by The Engine Room and local partners in Indonesia, Jamaica, Pakistan, and Uganda that show different types of digital ID systems that exist worldwide, as well as the issues and opportunities they create. The third and final section is the most important. "The People's Power" uses the metaphor of a fantastical beast to present a series of strategies for how to encounter, position, and respond to digital ID systems. It's the section where all of the information of the book gets translated into actions you can take and ways that you can move forward, depending on your own needs.

We've designed this guide to make sense when read chronologically, but we encourage you to approach it in whatever way you find useful. You can use the table of contents to jump to the sections that are most relevant to you, skip sections that you're already informed about, or work straight through the entire thing, completing all of the activities along the way.

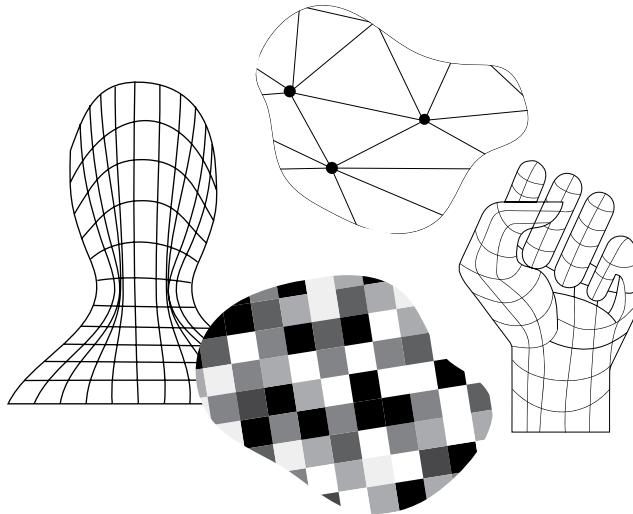
While most of the material that we cover here comes from the initial two reports written by The Engine Room, everything we know is because of experiences and lessons learned by our collaborators around the globe. From those organizing responses to the Aadhaar system in India to those making sense of NIDs in Jamaica, by learning from the expertise of our global collaborators we gain the strength and intelligence that we need to manage the different flavors of digital ID systems we face domestically.

Our hope is that this workbook leaves you feeling equipped to create your own responses and engagements around any digital ID systems you may find yourself facing. The best digital ID systems are systems that are equitable, and make life easier—not more challenging—for the people who use them. The only way to ensure that digital ID systems fulfill these conditions is to ensure that more of us are equipped to understand and advocate for the type of digital ID systems that best serve us. With this guide, we hope to support you wherever you are on that path.



"The best digital ID systems are systems that are equitable, and that make life easier—not more challenging—for the people who use them."

**MIMI ONUOHA AND MOTHER CYBORG
IN COLLABORATION WITH THE ENGINE ROOM TEAM**



Glossary

Throughout this workbook you'll see lots of different terms about technology, government, humanitarian organizations, and identification. This glossary provides more definition and context to those terms. We encourage you to refer back to this section while using the guide.

ADVOCACY ■ Efforts made in favor of a cause, idea, or movement. These can be carried out by allies or those who are directly affected by an issue. An organization working to make sure that digital ID systems are accessible to the elderly is *advocating* on behalf of that group.

BIOMETRIC DATA ■ Quantifiable and recordable measurements taken from people's bodies. Examples include: facial recognition, fingerprint scanning, voice recognition, and eye scanning. Because they come from living people's bodies, these measurements are unique to each person. They're also more permanent than passwords or analog identification for the same reason.

CIVIL SOCIETY ORGANIZATIONS (CSO) ■ Groups that provide support or engage in advocacy. CSOs can take many forms but they aren't tied to a government and don't operate for profit. They can range from small community groups to large nonprofit organizations. Many of the organizations we mention in this workbook are CSOs.

DIGITAL DATA ■ Information in an electronic form that can be processed, stored, and transmitted by a computer (as opposed to analog data, like a hand-written receipt on a piece of paper).

DIGITAL IDENTIFICATION SYSTEMS

(OR DIGITAL ID SYSTEMS) ■ Systems using digital technology to identify and verify individuals for a variety of purposes. These purposes range from public service delivery and aid distribution to national security. Digital identification systems go by different names around the world. For example, you may hear them referred to as "smart cards" in Bangladesh, as "national identification" in Jamaica, or as "e-ID" in Indonesia (the "e" stands for "electronic").

EQUITY ■ Justice or fairness that takes into account how different people may need different things to equally benefit. When we mention equitable systems in this handbook, we mean systems that are built to ensure that every person has what they need to survive, thrive, and succeed.

THE GLOBAL SOUTH ■ A term that refers to low and middle income countries, commonly referred to as 'developing countries' located in Latin America and the Caribbean, Africa, Asia and Oceania. The Engine Room has used the term in part to acknowledge political economy matters and realities, which are related – but not limited – to histories of colonization, domination, exploitation, inequity, etc.

IDENTIFICATION ■ The process of distinguishing and/or recognizing someone. Usually you are identified by someone else.

LEGIBILITY ■ The degree to which something is easy to read. Think of the example of how easy it is to read clear handwriting or how difficult it is to decipher messy or *illegible* handwriting. In digital ID systems, how well you and your identity can be read by the state is like handwriting: if a government can't make sense of your identity, then you are not very legible to it.

ORGANIZING ■ A method of social transformation that uses the collective strength of a group of people to address issues and make systemic change. Organizing is typically a process led by those directly impacted by an issue.

PRIVATE SECTOR ■ The part of the economy that is not funded by the government and instead is controlled by individuals or private organizations. Companies and corporations who produce items and services make up the private sector. Some of the major players in digital identification systems apart from governments are private sector tech companies that either design the systems or stand to profit from their adoption.

PUBLIC SECTOR ■ The public sector is the part of the economy that is funded and directly overseen by the government. In many countries, public education and national defense are part of the public sector.

QUALITATIVE DATA ■ Information that doesn't take the form of numerical values. This is usually gathered through conversation, surveys, questionnaires, experiences and observations. If someone asked you to record your dreams every day for a month, your responses—which would likely take the form of long answers or sketches—would be qualitative data. Your responses would be informative, though they wouldn't be able to be immediately passed through statistical or mathematical analysis like quantitative data.

QUANTITATIVE DATA ■ Information that takes the form of metrics or numbers. Quantitative data abounds because it is easy to use as a tool to compare, analyze, and organize data. It also helps computers to store, share, and function. Most digital ID systems use a mix of qualitative and quantitative data, with an emphasis on the quantitative.

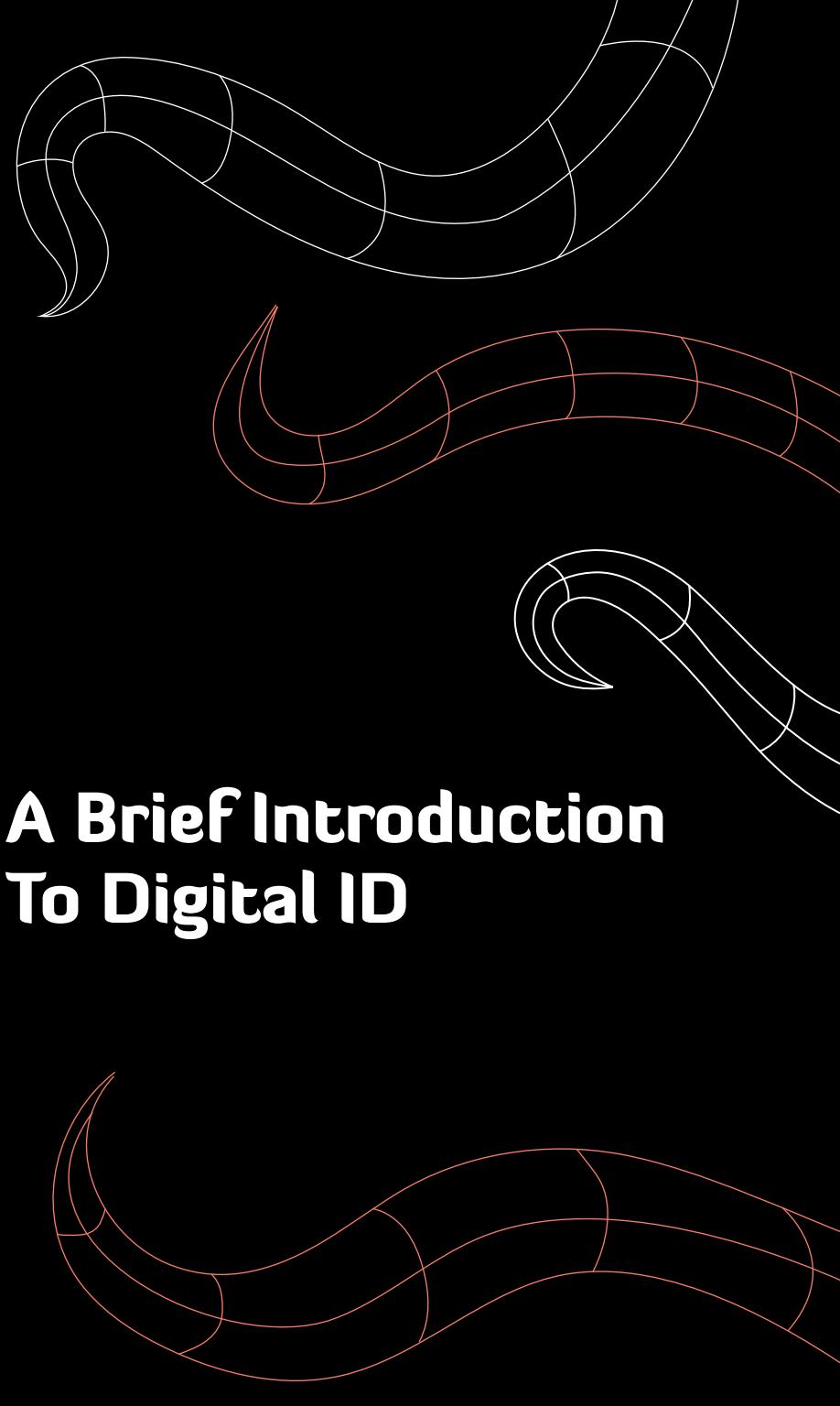
THE STATE ■ "The state" is an organized political entity of government that is tied to some land or territory. Often, the names of countries or the phrase "the government" are synonyms for 'the state. If you tell someone, "I'm going to India," they assume that you're going to visit the country. If you tell someone, "India is raising taxes," then they assume you're talking about the Indian state or the government.

States are typically centralized. In most countries there's one main national government—though it might be split into different departments or factions—and it does things like apply laws, impose and collect taxes, form treaties, engage in commerce with others.

People have always gathered in groups that craft ways of living together, but states as we know them today—centralized authorities that govern mostly settled societies of people—haven't always existed. This is important when it comes to digital ID, because we can see digital ID systems as an extension of states' interests in better understanding and tracking their residents (for reasons covering everything from taxation to protection).

THE UNITED NATIONS ■ Intergovernmental organization formed after World War II. Its purpose is to maintain international peace, security and good relationships among different nations.

VULNERABLE GROUPS ■ Groups of people who have fewer opportunities or less power due to circumstances and conditions outside of their control. For example, refugees are often considered a vulnerable group because they are understood to be fleeing their countries as their lives and/or livelihoods are in danger. Being in a vulnerable group doesn't remove any of an individual's personal agency or strength. Rather, it speaks to the structural difficulties different groups face as a result of things they cannot control.



A Brief Introduction To Digital ID



What Is Digital Identification?

Digital Identification combines two familiar terms: digital and identification (or 'ID' for short). Both are words immediately recognizable to most of us today, but combined they mean something more than the sum of their parts.

Digital refers to digital technologies, or electronic machines and systems that generate, store or process data.¹ The most well-known digital devices are computers and smartphones, but the term "digital" also includes the data that lives on and in these devices. Often phones, computers, and similar electronic devices connect to the internet, but they don't have to be internet-connected to count as digital.

¹ Victoria State Government, "Teach with Digital Technologies", 2019.

Identification refers to the process of identifying someone or being identified yourself. When you name who or what something is, you have identified it. You might identify someone by their bouncy walk or a brightly-colored hairstyle. Maybe you're able to identify when a family member comes home by the sounds they make as they enter.

In this workbook we refer to identification as the way the state—also known as the government of the nation you reside in—recognizes you as an inhabitant. This kind of identification is high-stakes. To be recognized by the government as a resident or citizen means gaining access to benefits like social services and legal protections. Identification by the state can also mean becoming exposed to additional responsibilities or dangers. Not all states protect or recognize all of their residents to the same degree, so how you are identified carries life-altering implications.

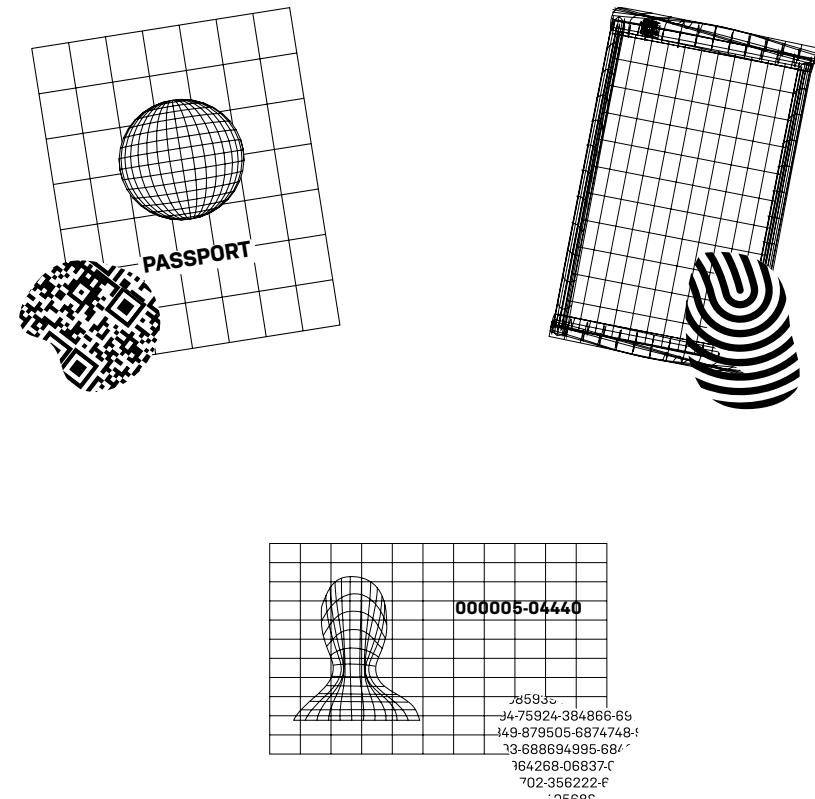
A hallmark of modern states is the desire to track citizens and residents. People who are properly tracked can be taxed, exempted or served, as well as policed and punished. Often governments intensify their desires to identify citizens when they are building and centralizing their own wealth or power. In other words, as the ambition of the state grows, so does the knowledge that the state needs to have about its residents.

Today, we are so used to systems of state identification that we hardly think about the many examples in our day-to-day lives: Birth certificates, social security cards, passports, military identification cards, municipal identification cards. Historically, documents like these have been paper-based, and many of them still are. If you flash your driver's license to get into a bar, you're presenting a physical (not digital!) mode of identification. Your driver's license isn't entirely divorced from digital systems since the information that produced the license is likely stored in a

digital database.² But you know the license itself isn't digital because you can physically hand it over to get into the bar. It isn't something that you show on a screen or device.

Your individual driver's license also isn't directly tied to your other identification cards (if you lose your driver's license, you'll still have your birth certificate). But these forms of identification are still linked even though they're separate documents: To get your first driver's license, you might have needed to show your birth certificate. This web of connection is one that digital ID systems aim to make even smaller. In a digital ID system, all of your forms of identification are directly tied to each other. Digital ID systems use digital technology to identify and verify individuals under one number, entry, or identifier. In doing so, they either eliminate the need for different forms of identification, or ensure that those forms of identification are tightly linked together in a way that is impossible with analog systems.

Connecting so many different types of information isn't a straightforward task. Digital ID systems are often accompanied by biometric data collection to help accomplish the linkage. Biometric data are unique measurements taken from people's bodies. Some forms of biometric data, like fingerprint scanning, have been around for decades. Other forms, like facial recognition and iris scanning, are more recent. Biometric forms of data are unique to every individual and once they've been collected, the data is permanent. The combination of uniqueness (no one else has your fingerprint) and permanency (your fingerprint will never change) is what makes them ideal for identifying people in a long-lasting way.



2 Note that in many countries, driver's licenses actually do contain digital information in them. In the US, they operate as a sort of middle ground, a physical device that mostly are representations of digital information. The world of digital ID isn't straightforward!

If you've ever had to show something on your phone to be allowed into a country, building, or plane, then you already have direct experience with a form of digital identification. But we are mainly focused on national digital ID systems in this handbook. These types of digital ID systems typically involve a government (as opposed to a private company or organization) storing its residents' information in electronic servers and databases.

We've created this handbook because digital ID systems are on the rise. Over the past two decades they have become more and more popular globally. Governments in countries including Bangladesh, Ethiopia, Nigeria, Zimbabwe, Thailand, Indonesia, Jamaica, Pakistan, Uganda, Kenya, Cameroon, Ecuador, Jordan, Kyrgyzstan, Iran, Senegal, Turkey, the Philippines, and India have all implemented or begun administering national digital ID systems. Each of these systems is different, and though we refer to them as "digital ID" in this handbook, in your own country or context the equivalent system might be called a "smart card", "electronic ID", or something completely different.

Whatever their name, all of these systems have basic things in common, including identifying individuals and linking their access to other services—like opening a bank account, voting, getting a job, accessing education or healthcare, or even buying a SIM card for a mobile phone—to their digital ID.³

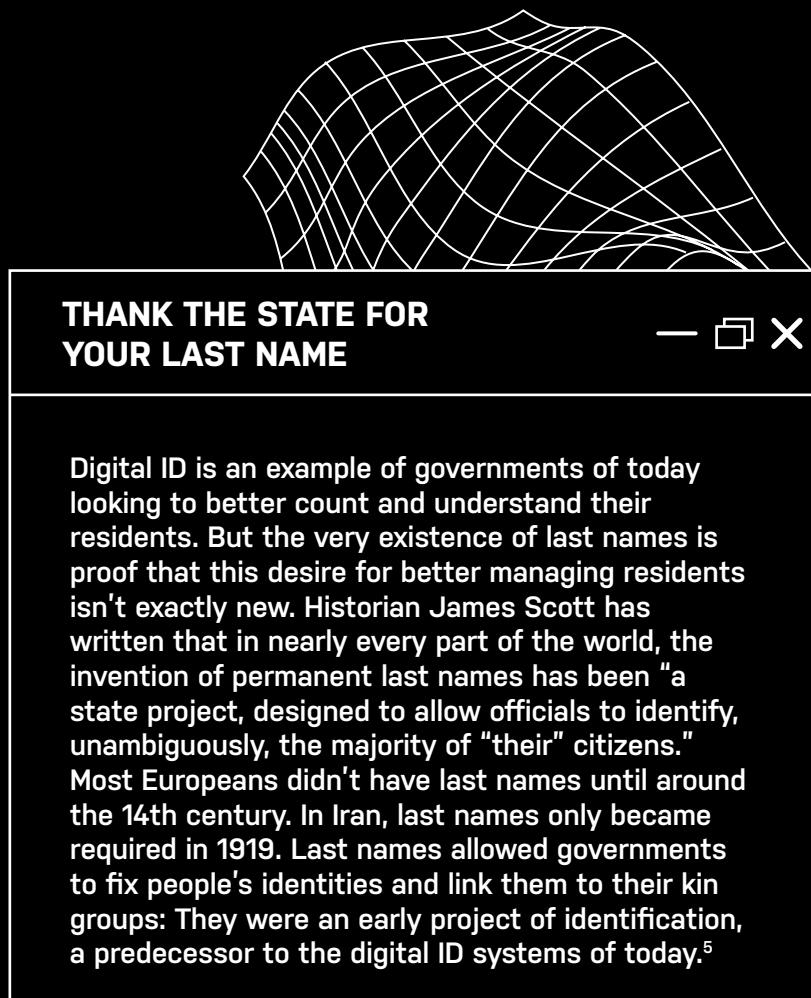
Researchers say that digital ID systems are perceived as being "more efficient and effective than their (largely paper-based) predecessors. They also pervade more domains of people's everyday activities than previous systems."⁴ In other words, digital ID systems become embedded into more parts of our lives

than paper-based identification. They are seen as more inclusive, better at creating links to other forms of identification, and easier to access than other systems. As we'll see later on in this workbook, existing digital ID systems have lived up to this reputation for some people, but not all.

Given their growing prevalence and how much is wrapped up in the process of creating and using digital ID systems, it's crucial that we all understand what these systems are and how to navigate them.

³ Sara Baker and Zara Rahman, *Understanding the Lived Effects of Digital ID*, The Engine Room, 2020, 8.

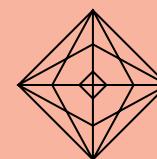
⁴ Janaki Srinivasan and Elisa Oreglia, "The Myths and Moral Economies of Digital ID and Mobile Money in India and Myanmar," *Engaging Science, Technology, and Society* 6 (2020): 215–36.



**THANK THE STATE FOR
YOUR LAST NAME**

— X

Digital ID is an example of governments of today looking to better count and understand their residents. But the very existence of last names is proof that this desire for better managing residents isn't exactly new. Historian James Scott has written that in nearly every part of the world, the invention of permanent last names has been "a state project, designed to allow officials to identify, unambiguously, the majority of "their" citizens." Most Europeans didn't have last names until around the 14th century. In Iran, last names only became required in 1919. Last names allowed governments to fix people's identities and link them to their kin groups: They were an early project of identification, a predecessor to the digital ID systems of today.⁵



Activity 1

From Identity to Identification

This activity will guide you in unpacking what makes up your core identity, how that translates into forms of data, and how that data is used for identification. Having a sense of these processes will make it easier to see the logic behind analog and digital identification systems.

What happens when the complexity of identity is stripped down to simple characteristics like the color of your eyes, your weight, and where you live? What gets lost in translation and how does this affect your ability to navigate the world?

⁵ James Scott, "State Projects of Legibility and Simplification", *Seeing Like A State*, 1998.

Imagine that you're sitting at a cafe. A stranger sits down next to you and strikes up a conversation. As you are sharing stories, they ask you, "What do you spend most of your time thinking about?"

How do you respond?

The conversation continues and you realize that the two of you share a lot in common. Though you've only just met, this person begins to feel like someone you have known your whole life. They ask you to share how you would describe yourself in person versus how you would describe yourself online. You feel comfortable enough to be candid with them.

What parts of yourself do you highlight when first encountering this person? How is this different from what you share when first meeting someone online?

Most of the information that you've shared with your new friend is likely *qualitative data*.

Qualitative data is information gathered through conversation, experience, questionnaires, interviews and observation. It's also known as unstructured data because it can be difficult to measure or analyze. Qualitative data is often contrasted with *quantitative data*.

Quantitative data is data that can be counted, or usually takes metric form. Everyday examples of quantitative data are your height, the numbers that make up your credit score, or test scores. This data is structured and numeric. It can easily be analyzed, compared, and represented digitally.

Digital ID systems include both quantitative and qualitative data. Your name is qualitative; your height is quantitative. Qualitative identifying information gives us lots of information in our personal lives, but it also tends to change more easily and be less precise than quantitative information. This is one of the reasons why our digital ID systems tend to involve lots of quantitative information (think about how governments give out identification numbers to their residents, not identification words).

The tension between *quantitative* and *qualitative data* underscores the major difference between identity and identification. The identity that you hold might change over time. You might have one favorite food today and change your mind tomorrow. The hobbies that once defined you might switch to include others as you grow older. We might put more personal emphasis on the rich qualitative data that defines us, but our governments are more interested in the rote facts that are constant and don't change over time. The task of identification is made easier when the information being tracked remains constant and precise (if you've ever had to legally change your name, then you know this firsthand). The very aspects that make qualitative data more engaging to us are what make it more troublesome for national identification systems.

"The best way to do that is to turn to communities who have already had to face these ramifications by the sole fact of their countries having been earlier adopters or digital ID systems."

Why Digital Identification Systems?

Why are so many countries implementing digital identification systems? What are the advantages to using these systems for the state and the people being identified?

The Engine Room's research has shown that governments implementing Digital ID systems often give the following five reasons for why they use them:⁶

⁶ Baker and Rahman, "Understanding the Lived Effects of Digital ID", 27.

1. **To ensure people have acceptable identification to access services.** Many states believe that combining identification for multiple services into one digital file will make life easier for both the government and the population by streamlining the number of verification documents needed for daily life.
2. **To provide necessary services more quickly and effectively.** Such services range from voting and financial assistance to food rations and international protection for refugees. Once again, combining data is intended to reduce the friction necessary to access these services.
3. **To give people excluded from financial institutions access to bank accounts and financing.** In this case, digital ID systems are intended to act as a kind of bridge, creating access for those who have been previously unable to reach certain services.
4. **To connect services that enable easier transactions amongst a variety of government, CSO and private sector actors.** Merging discrete systems doesn't just decrease the number of IDs people must carry, but also supposedly improves government efficiency by cutting out systems doing duplicated work.
5. **Improve public safety and decrease fraud.** This justification doesn't address the underlying causes of crime, theft, and other public safety concerns. Despite this, some governments have insisted that if everyone is accounted for, crime and fraud will be disincentivized because any threats to public safety can be tracked down.

The five reasons above all follow a similar theme: they focus on making life easier for residents and their governments. The idea of simplification is the biggest reason why digital ID systems continue to exist. In the best case scenario, they are intended to be a kind of win-win that makes everyone's lives easier.

Governments that can account for and reach all of their residents whenever they want are governments that have more power to enforce financial, security, and policing aims. But there are also many examples of individuals who have found having enhanced control over their identities to be incredibly powerful. In Bangladesh, being identified as a freedom fighter (someone who fought in the Liberation War in 1971) is a valuable identity to hold. In Ireland, the Gender Recognition Act allows those over the age of 18 to legally change their gender identity through self-determination, thus empowering transgender people to be legally recognized by the state. And in Senegal, women who are sex workers are given identification cards that entitle them to free health care, condoms, and education initiatives.⁷

On the other hand, whether digital ID systems are helpful for citizens or not largely depends on the circumstances, the characteristics of those systems, and who is in power. As an Engine Room report showed, "In Afghanistan, the Taliban took charge of biometric databases left behind by the US forces, possibly endangering thousands of people who worked with the US during the 20-year occupation".⁸

Unfortunately, there are many more examples of mismanaged digital ID systems becoming reality. In Bangladesh, biometric data collected from Rohingya refugees by the United Nations High Commissioner for Refugees was shared with the Myanmar government. In other words, the same military that conducted the most recent genocide against the Rohingya now holds the biometric data of the very population it tried to eradicate. "Bangladesh then used the information, including analog photographs, thumbprint images, and other biographic data to submit refugee details to the Myanmar government for possible

repatriation."⁹ This event showed the danger of the increased power to surveil and catalog that digital ID systems bring with them." In all of these cases, the government's access to digital ID databases is precisely what gave them the power and ability to inflict harm on different groups.

Furthermore, it isn't just governments that are involved in the task of creating a national ID system. Private companies are often contracted to build out these ambitious digital systems. The companies benefit financially from the contracts but add another layer of complexity to the system.

Regardless, digital ID systems continue to expand in their use and their reach. Our task, then, is to understand the concrete ramifications of these systems so that we can balance all of the different potential outcomes that they can bring. The best way to do that is to turn to communities who have already had to face these ramifications by the fact of their countries having been earlier adopters of digital ID systems.

7 Zara Rahman, "Digital ID: Why It Matters, and What We're Doing about It | The Engine Room," 2018.

8 Quito Tsui, and Teresa Perosa, Digital IDs Rooted In Justice, The Engine Room, 2022.

9 Tsui and Perosa, Digital IDs, 2022.

DIGITAL ID TAKES ON THE WORLD

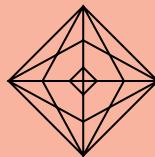
From Kenya to Turkey, part of the reason why digital ID systems are increasing in popularity is because the forces fueling their global adoption stretch beyond borders:

International Goals - One of the 2015 international goals that the United Nations has adopted is to provide legal identity for all people by 2030. For many countries, Digital ID has been the solution, made even more possible by the willingness of the World Bank to funding digital ID systems in places like Nigeria.

Technological Advancement - We live in a digital age, and governments are becoming just as fluent as everyday people in gaining information through devices and screens. In the global South especially, digital ID systems are seen as a solution to corruption, inefficiency, and security threats. Creating them taps into the powerful (if unproven) assumption that technological solutions can quickly change deeply-rooted social practices.

Profit Motives - Some estimates say that the identity verification market is set to double from \$7.6 billion in 2020 to \$15.8 billion in 2025. There's a lot of money to be made in the field—not to mention lots of data to gather—which is why so many companies have jumped into the game. In Zimbabwe, a 2018 proposed partnership with Chinese artificial intelligence corporation CloudWalk Technology was intended to allow the company to have access to a database of Zimbabwean faces which they could then use to improve the accuracy of their facial recognition technology. When corporate interests meet mandatory state data collection without data privacy laws, corporations nearly always stand to gain.

Covid-19 - Though the Covid-19 pandemic has been differently felt in different parts of the world, the reduction in in-person gathering has strengthened the push for digitized systems overall. In the US, vaccine passports have emerged as a limited case of sector-specific digital ID. Vaccination passports are used to confirm whether residents are vaccinated, have recovered from Covid-19, have received booster jabs, or have tested negative for the virus.



Activity 2

Where Digital ID Meets You

Use the grid below to see if and how digital ID systems show up in your life.

What are places or experiences that require your identification in order for you to access them?	What services do these places and experiences give you access to?	What is at stake if you do not have the required identification?	Is this identification accessed in digital or in physical form?

Which items, if any, in this list of identification are only accessible in digital form?

The digital ID systems that you interact with may be different from the ones we are investigating in Indonesia, Jamaica, Pakistan, and Uganda. Across varying contexts and situations, all digital ID systems highlight the ways that IDs can often grant you access to spaces and benefits.

Moments when you are denied access can be revealing in a completely different way. These moments can point out the structure of the systems that you are interacting with. Use the prompts below to examine a time you were denied access to a place, person, or experience and see if you are able to point out what could have been different.

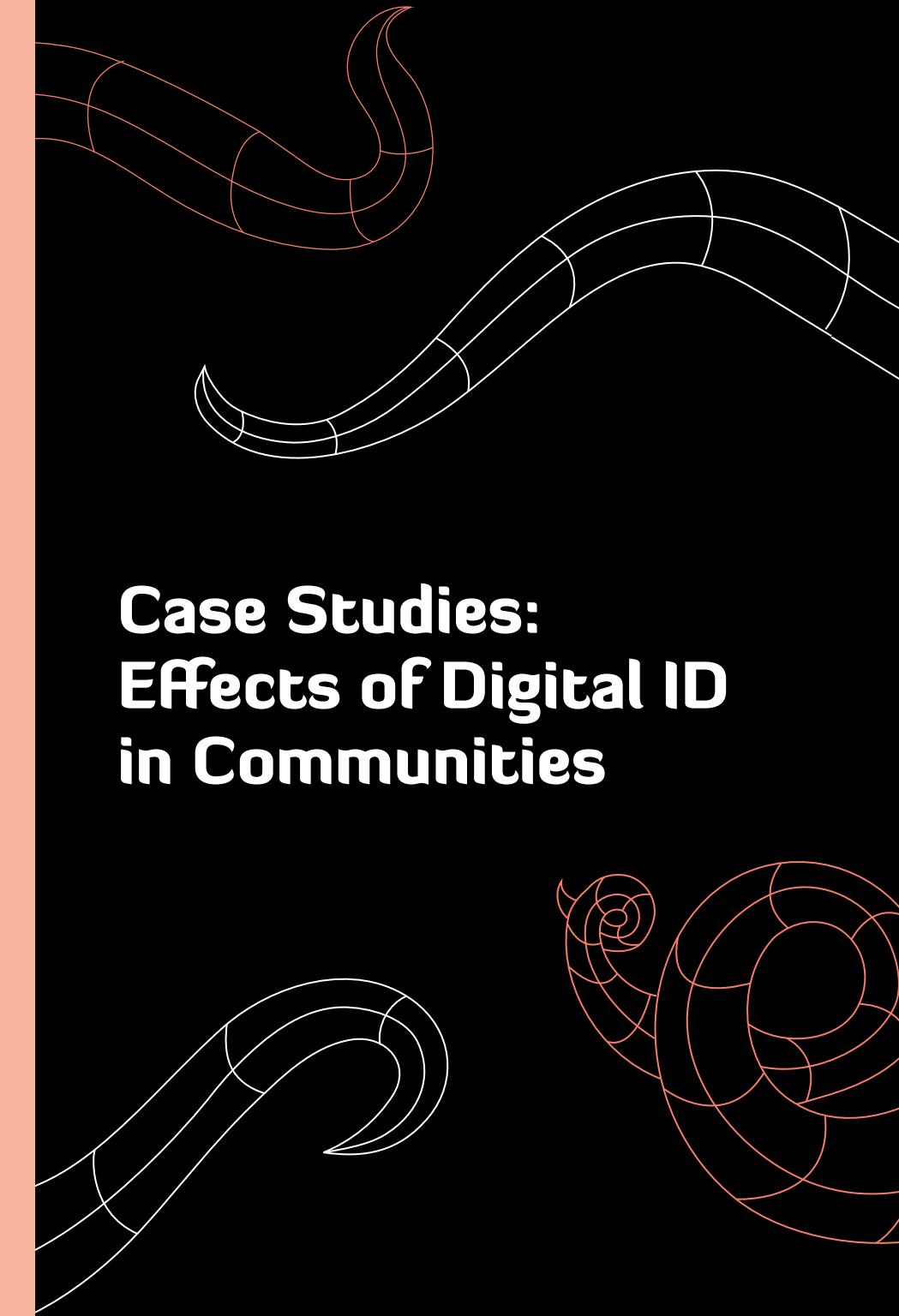
Describe a time in which you were denied access to something because of not having the proper identification.

(If you have never been denied access due to lack of identification, consider what services other people in your community have been denied because of digital ID and use that as your perspective for answering the following questions.)

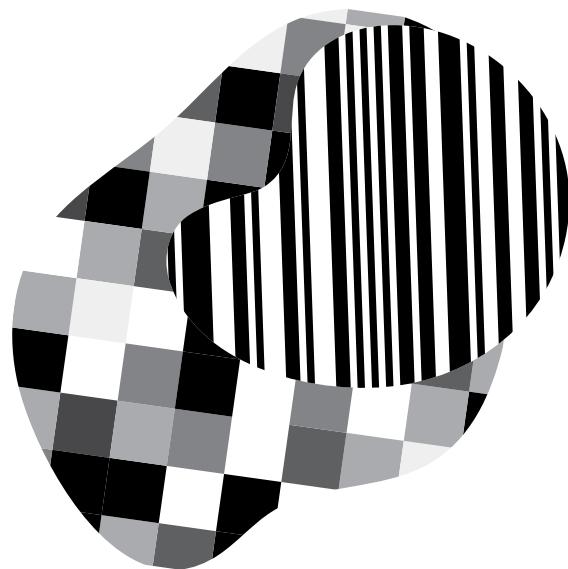
How were you able to overcome this obstacle?

Did anything change after this incident? Did you start doing something differently?

What is your strategy for handling moments when you could be denied access to places or services?



Case Studies: Effects of Digital ID in Communities



Case Studies: Effects of Digital ID in Communities

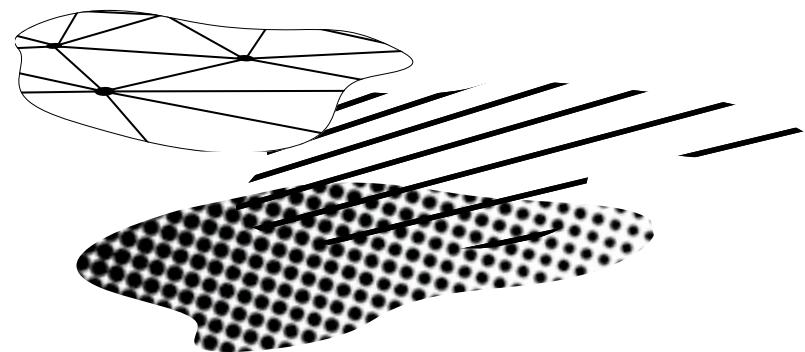
How concerned should we be about digital ID systems?

The best way to answer this is to look at the lived experience of those who have already had to navigate these systems in their countries. In this section, we focus on Indonesia, Jamaica, Pakistan and Uganda. These four countries have very different types of digital identification systems, and together they help flesh out the story of the many different forms national digital ID systems can take.

In each country, the Engine Room partnered with local researchers familiar with the national context (you can see more about how they conducted the research in our appendix). Collectively, the systems span a long period of time. Among the four countries, Pakistan's system (introduced in 2000) is the oldest, whereas Jamaica's was introduced in 2017 and ratified in 2021.

Though the systems are different, looking at them together also shows some clear similarities that are common across most digital ID systems: all of them were introduced by the state onto the residents; all of them are required for residents and citizens to access crucial services; and as much as they have streamlined certain aspects of social life, they have also introduced difficulties in others.

As you're looking at the different systems, see if you can find any other similarities and differences among them.



Country	Indonesia	Jamaica	Pakistan	Uganda
Name of Digital ID System ¹⁰	Kartu Tanda Penduduk Elektronik (e-ID card or e-KTP)	NIDS	NADRA - National Database and Registration Authority System.	Ndaga Muntu Consists of National ID Number (NIN), and the National ID Card (NIC)
Date Introduced	2009	2017	2000	2015
Information Collected	<p>Personal data including:</p> <ul style="list-style-type: none"> Gender Marital status Disability information Religion <p>Biometric Data including:</p> <ul style="list-style-type: none"> Fingerprints Iris scans Blood type: <p>Residents must present both an e-ID and a Family identification card.</p>	<p>Personal data including:</p> <ul style="list-style-type: none"> A facial image - Reference numbers that track the user's taxpayer registration number, passport number, and national insurance number Fingerprints Manual Handwritten signatures 	<p>Personal data including:</p> <ul style="list-style-type: none"> A photograph Fingerprints <p>Required IDs:</p> <ul style="list-style-type: none"> Computerized National Identity Card (CNIC) 	<p>Personal data including:</p> <ul style="list-style-type: none"> Birth certificate Marriage License <p>Biometric Data including:</p> <ul style="list-style-type: none"> Fingerprints Facial Scans
Information Used For	<p>Access to public services such as:</p> <ul style="list-style-type: none"> National healthcare Public education State benefit programs. <p>Registration is also required for voting.</p>	<ul style="list-style-type: none"> Verifying an individual's identity Facilitating electronic signing of documents Accessing government services online¹¹ 	<ul style="list-style-type: none"> Social welfare programmes Voting and bank accounts SIM card Paying utility bills Accessing education and healthcare COVID-19 testing and vaccination 	<ul style="list-style-type: none"> Healthcare Financial assistance Social welfare programmes Bank services such as loans In some cases, applying to jobs
How Data Is Stored or Managed	Centralized database maintained by the Ministry of Home Affairs.	No information yet available on how data will be stored and managed for NIDS. ¹²	NADRA was built in 2001, and is based on local servers stored at NADRA's own facilities.	The National Identification and Registration Authority plans, implements and rolls out the digital ID system.

¹⁰ This data was gathered by The Engine Room in collaboration with researchers (Stacey-Ann Wilson and Amma Khan) and organizations (ELSAM and Policy) from each of the respective countries.

¹¹ Patterson, Chris, "House Passes Nids Bill." Jamaica Information Service, 2022.

¹² "NIDS Will Have Strongest Database Protection System in Jamaica, Says Green," Jamaica Observer, 2022.

Indonesia	Combined, what does this information tell us about who a person is?	What does the type of data collected tell us about the priorities of this system?
Gender		
Blood type		
Marital status		
Disability information		
Religious affiliation		
Iris scan		
Full set of fingerprints		



Activity 3

Digital ID Systems Around the World

Look at the different data each of these digital ID systems collect. Try to get a sense of what types of stories the data tells about a person. Can you tell what the priorities of each system are based on the data collected? Consider what each type of data means to each country. How does this data shape a story about participants in the system, and the system itself?

Jamaica	Combined, what does this information tell us about who a person is?	What does the type of data collected tell us about the priorities of this system?	Uganda	Combined, what does this information tell us about who a person is?	What does the type of data collected tell us about the priorities of this system?
Handwritten signature			Marriage license		
Taxpayer registration number			Fingerprints		
Passport number			Facial scan		
National insurance number					
Pakistan	Combined, what does this information tell us about who a person is?	What does the type of data collected tell us about the priorities of this system?			
Full set of fingerprints					
Digital photograph					

Living with Digital ID

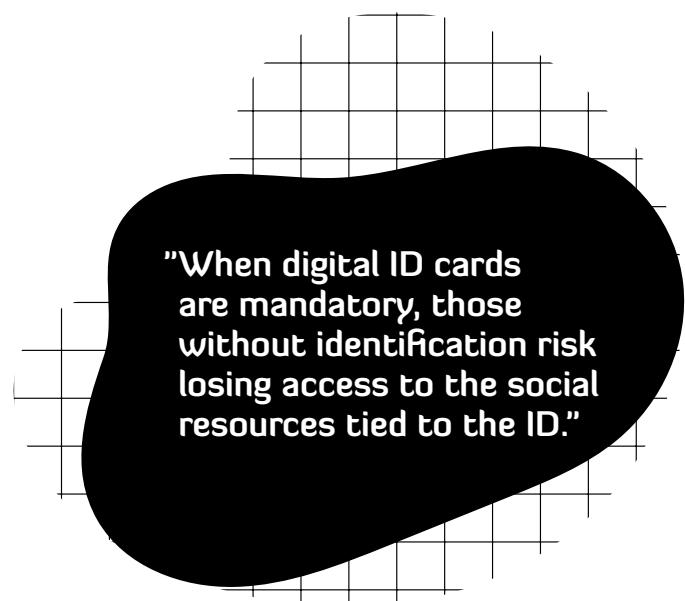
When digital ID systems have created obstacles for residents, it is typically those with the least social, legal, and financial protections who are most impacted. For example, women who live in intensely patriarchal societies, rural farmers who must travel large distances to access required registrations, and transgender people who deal with harassment at the perceived distinction between legal name and gender expression are all vulnerable groups. The challenges that these groups face tend to fall into one of three categories: **access, privacy and data**, and **governmental inefficiency**.

We believe that the true test of whether a system is working is how it affects those who have the most to lose. A digital ID system that protects those who need the most protection is a digital ID system that is working in service to all.

The ubiquity of these shared challenges suggests that those responding to issues within digital ID systems should be on the lookout for similar problems.

Access

Mandatory digital ID cards mean that those without identification risk losing access to any social resources tied to the ID. Issues of access always have the same things in common: the way that registration for a system is set up makes it so that the task is disproportionately harder for certain people.



The table below goes over some of the issues of access present in Indonesia, Jamaica, Pakistan, and Uganda's digital ID systems.

Indonesia

Those registering need to have a family card, which in practice means that women need the permission of their husbands to access services.

Victims of violence who move from one place to another struggle to provide enough documentation to verify their identity.

Disabled people have also struggled with barriers to obtainment.

Indigenous minority communities in Indonesia with faiths other than Muslim, Christian, and Hindu need a declaration from an official organization representing their community even though not all indigenous communities are organized in such a way. An indigenous rights advocate estimated that over 1 million people from these communities don't have an e-ID card for this reason.

Jamaica

NIDS enrollment process requires providing extensive information, and if an applicant cannot provide one or more of the needed pieces of information, the authority is empowered to decline enrollment.

A Constitutional Court found that the NIDS process was intrusive.

Pakistan

NADRA is the oldest system of these four, and the most embedded in everyday life. Supposedly registration in the system is voluntary, but because it is widely required for civic life it is essentially mandatory.

The system is patrilineal, so it ties women's citizenship to their male relatives and makes women reliant upon these men. Currently an estimated 12.48 million women lack an ID card (CNIC).

Though trans and khawaja sira¹³ people have the right to self-identify on their identity cards, they still face discrimination in their interpersonal interactions with bureaucrats at registration offices.

Ethnic minorities have been discriminated against through NADRA. Afghan refugees were previously subject to a parallel system of identification, and have only recently been able to register for an identity card. Those with complex identities, like migrants, have reported issues of not having their citizenship status recognized.

Uganda

Across the board, interviewees and focus group participants indicated that the implementation of the digital ID system in Uganda worsened issues of access to social services like healthcare and banking access. Registration materials are available only in English, and not in any local language. Six years into implementation, it is estimated that up to one-third of Uganda's adult population still lacks a national ID card.

The system is heavily centralized. There are no NIRA regional offices. Digital ID matters are handled by desks in select districts located within local authorities' offices. This requires people to travel long distances both to register and to collect their ID cards.¹⁴

Errors in the registration process have also left some elderly people excluded from essential social welfare programmes.

-
- 13 Khawaja Sira is an umbrella term used to describe local gender-variant identities in Pakistan. Given the legacy of colonialism in the country, many of the terminologies used globally (eg. transgender) do not map onto local manifestations of gender and sexuality..
 - 14 Tsui and Perosa, *Digital IDs*, 2022.

Below are issues that arose in each country. What structural or social procedures could be implemented to prevent a similar outcome in your own country or area? Who would need to be responsible for those procedures?

Indonesia: Victims of violence who move from one place to another struggle to provide enough documentation to verify their identity.

Jamaica: The digital ID enrollment process requires providing extensive information, and if an applicant cannot provide one or more of the needed pieces of information, the authority is empowered to decline enrollment.

Pakistan: Though trans and khawaja sira people have the right to self-identify on their identity cards, they still face discrimination in their interpersonal interactions with bureaucrats at registration offices.

Uganda: Errors in the registration process have also left some elderly people excluded from essential social welfare programs.

“The more sensitive the data, the more important the answers to these questions.”

Privacy & Data

National ID systems rely upon the collection of huge amounts of data. Significant data collection prompts important questions:

*What types of data are collected?
Where does the data live?
How long is it stored?*

The more sensitive the data, the more important the answers to these questions. You might not care very much if someone hacks into a database that contains information about what you ate for dinner two weeks ago. But if there's a data breach in a database that contains your financial and national identity information, you have justifiable reason to be worried.



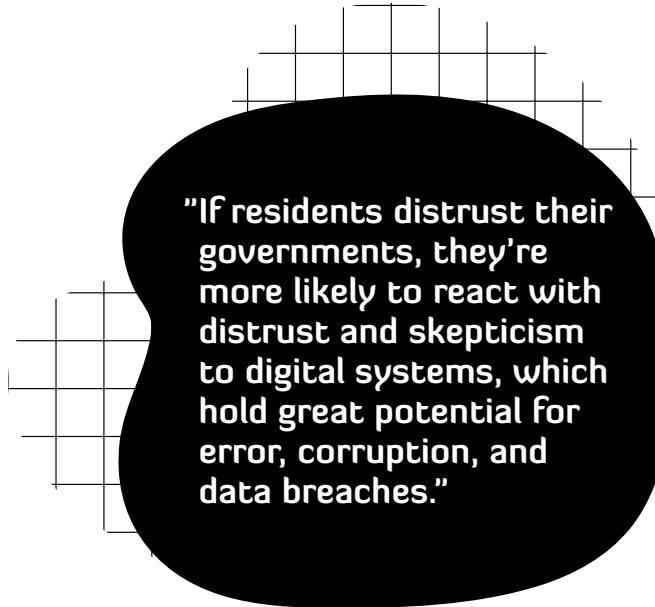
In the table below, you'll see the specific problems around privacy and data faced in Indonesia, Jamaica, Pakistan, and Uganda:

Indonesia	Jamaica	Pakistan	Uganda
<p>Indonesia's e-KTP requires the collection of more than 30 data points. Data is shared with 54 government agencies and 3400 private agencies. Citizens don't know what data is being shared. There's no clear transparency around how data is shared and with whom. The country has seen serious data breaches that have only made the problem worse.</p>	<p>Entities within the Jamaican justice system like the Major Organised Crime and Anticorruption Agency have sought access to NIDS, which amplifies fears of misuse from the public.</p>	<p>The data stored within the NADRA system is widely believed to be insufficiently secure — based on the government's historical failures to keep data secure or to prevent misuse.</p> <p>However, the biggest privacy concern remains the lack of legislation regarding data protection, meaning that "one of the world's largest centralized citizen databases" lacks the legal protections necessary to ensure that its data is secure¹⁵.</p>	<p>Registration requires the provision of a substantial amount of personal information. Citizens are not given any explanation as to why the data is being collected and are not told how it is to be stored, managed, or protected.</p> <p>This raises concerns that the information might be misused or subject to data breaches. Participants report fears that their information will be used in fraud or extortion schemes. Communities are concerned they will be subjected to political violence.</p>

15 Tsui and Perosa, *Digital IDs*, 2022.

Take a moment to reflect on one of the above country's issues around data and privacy. What safeguards would need to exist to make sure that the same issue wouldn't repeat itself in your own country or region?

Consider all the parties who play a role in implementing a digital ID system, from government officials to regional offices to community representatives to the developers who create the digital infrastructure. Who would need to be a part of the effort to put your brainstormed safeguards in place?



"If residents distrust their governments, they're more likely to react with distrust and skepticism to digital systems, which hold great potential for error, corruption, and data breaches."

Governmental Inefficiency

Governments (and their relationships with the private sector companies that they often partner with) present some of the biggest problems when it comes to the implementation and citizen response to digital ID Systems. These issues include bureaucracy, corruption, lack of transparency, zero consultation, and even embezzlement.

National ID systems are always carried out by governments. The more that citizens trust their governments to represent them fairly, the more willing they are to accept national digital ID systems that their governments announce. The reverse is true too: if residents distrust their governments, they're more likely to react with distrust and skepticism to digital systems, which hold great potential for error, corruption, and data breaches.

Below are specific issues around governmental distrust in each of our case study countries. Read about the problems and devise your own solutions. What would you do to make the digital ID system more equitable?

Indonesia

More than 80 public officials reportedly were involved in an embezzlement scheme which stole over a third of the \$440 million destined to fund the digital ID system. This lowered trust in the government's ability to regulate and protect resident's information.

Jamaica

Many Jamaicans' have a low level of trust in their government. A history of unfulfilled promises has contributed to a feeling of significant skepticism towards the state.

Government was accused of rushing the NIDS legislation through parliament and leaving little opportunity for consultation. The government claimed that the need to secure loans worth \$68 million from the Inter-American Development Bank, which contributed to the haste of the process.¹⁶

Many civil society organizations, as well as the main opposition party, were left frustrated by the lack of engagement.

Pakistan

In many instances, Pakistani citizens are not told how their information is used. Much of NADRA operates without the informed consent of the public. There is no disclosure regarding who will be using the data, what the data will be used for, or how access to the data is authorized.

NADRA is being used by the government for ever-expanding purposes, from identifying potential beneficiaries of public services to finding individuals who may be subject to taxes.

Uganda

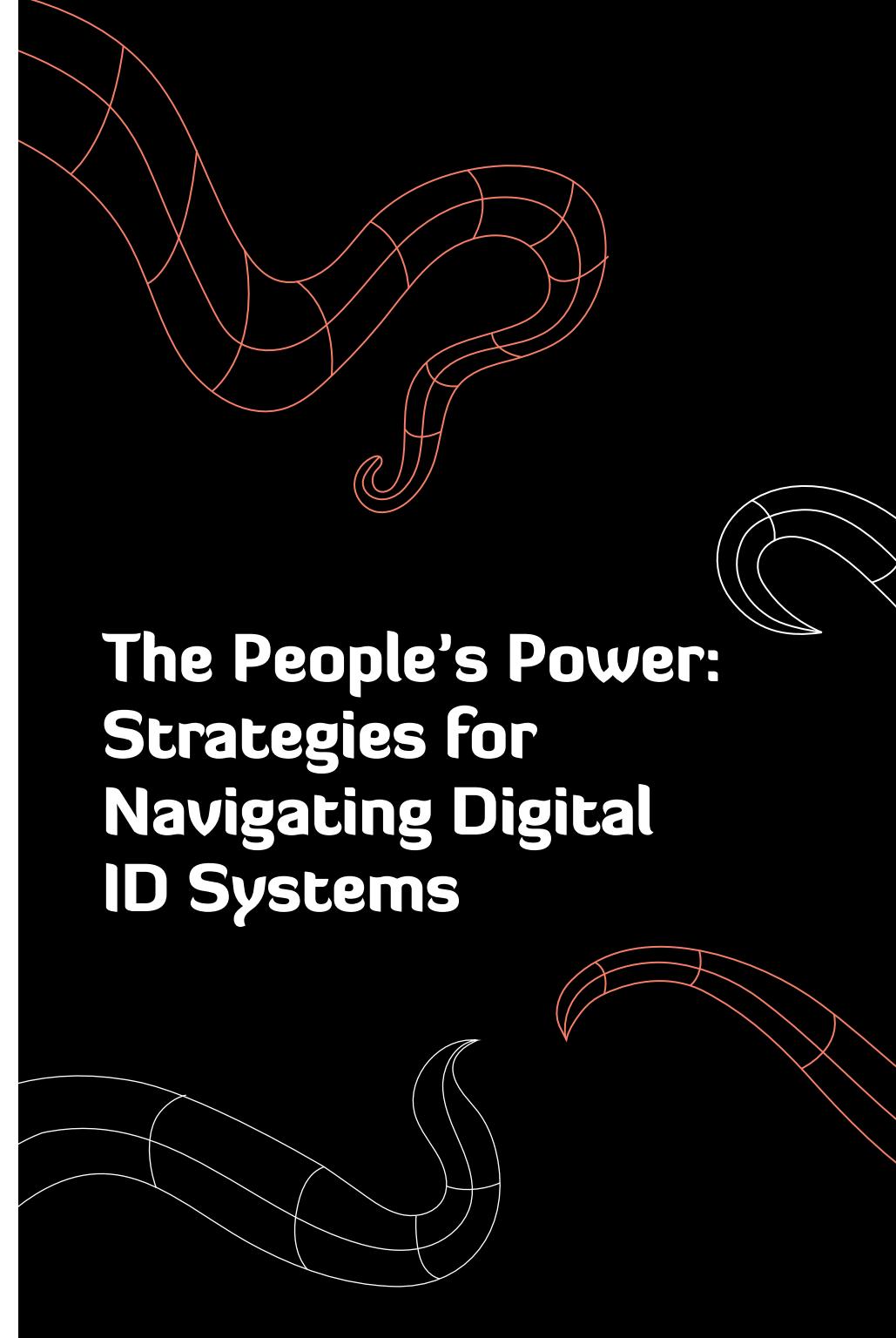
One of the main grievances voiced by research participants was related to the government's lack of consultation, and the absence of civil society involvement in the design and implementation of the Ndaga Muntu system.

There is an overall perception that many of the problems and gaps people now face when interacting with the system, especially those coming from marginalized communities, could have been solved (or identified from inception) had civil society been consulted.

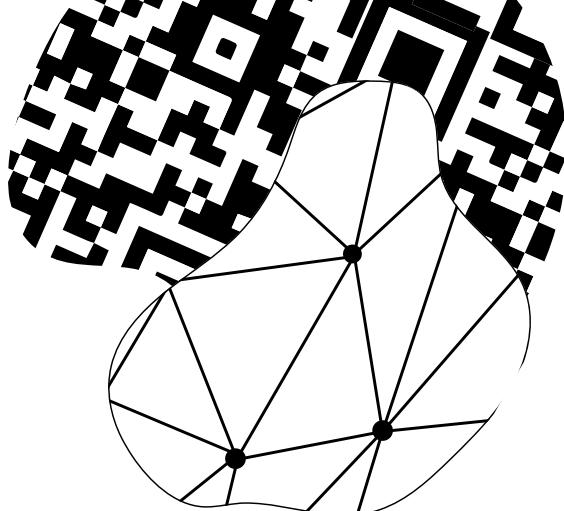
While getting the national ID can take months or even years, one can register and obtain a driver's license in Uganda in just one day.

Every challenge provides an opportunity, even though that opportunity may require time and perspective to identify. Looking at the ways governments have failed in the deployment of digital ID systems in each country, where are there opportunities for you and your community to intervene and ensure the development of digital ID systems that avoid previous pitfalls?

What resources, conditions, or support would you or your community need to prioritize those opportunities?



The People's Power: Strategies for Navigating Digital ID Systems



The People's Power: Strategies for Navigating Digital ID Systems

Properly functioning digital ID systems should work for us all. They should ensure safety, privacy, and be easy to access. If these systems become more burdensome than empowering, then it is up to everyday people—students, educators, workers, grassroots activists, civil society advocates, and more—to come up with strategies to change them.

In this section, we present three frameworks for advocacy and organizing around digital ID systems. These frameworks are not intended to be exhaustive, but they are designed to spark inspiration and provide a sense of direction. Whether you're in a country that has never publicly considered such systems or you've grown up with one, it's never too early or too late to think deeply about what type of relationship with digital identification you and your community want to have.

We've taken inspiration from the recent report, "From Data Criminalization to Prison Abolition" published by the Community Justice Exchange. In their report, the Community Justice Exchange imagines key federal data systems and departments in the United States as fantastical beasts.¹⁷ Rendering complicated systems as beasts makes it easier to concretely illustrate their unique characteristics and reach.

By depicting digital ID systems as a multi-limbed beast, we aim to use a similar approach and make these large and complicated systems easier to conceptualize and manage. Using the organizing and advocacy work in Indonesia, Jamaica, Pakistan and Uganda, on the following pages we present exercises that can help you determine how to strategize around digital ID systems that you might face.

We're intentionally focusing on what is possible, not just what has happened in the past. Our ultimate goal is to illuminate the many choices you have when coming face to face with an overwhelmingly large and complex structure. Digital ID is, after all, just one of such systems.

¹⁷ Community Justice Exchange, *From Data Criminalization to Prison Abolition*, 2022.

Encountering the Beast of Digital ID: Frameworks for Approaching Digital ID Systems

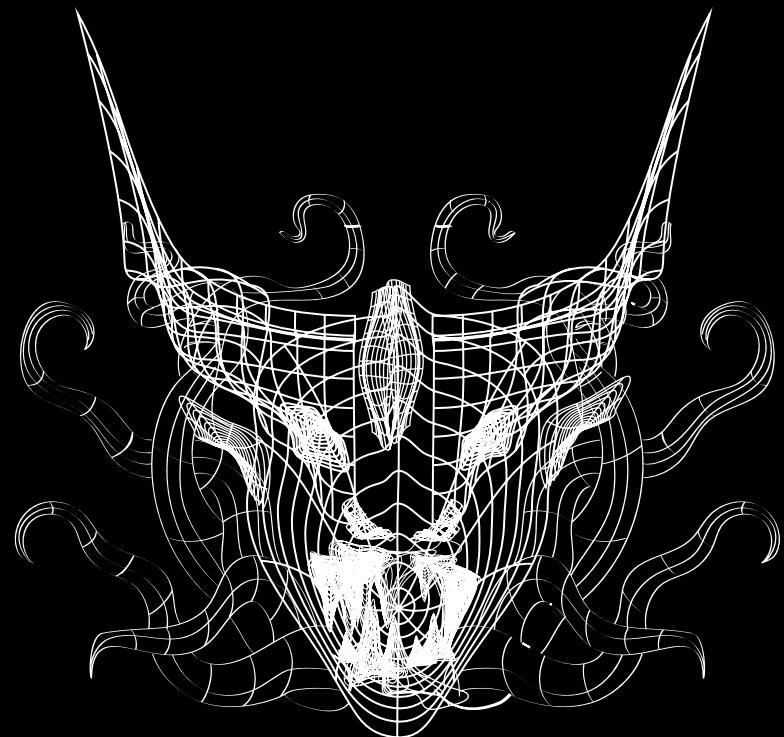
Imagine you are walking along a path when you suddenly encounter a large beast. The beast has horns and claws on the end of long, scaly limbs. It swings several tentacles in a circle over its head as it huffs down at you. This is the fabled Beast of Digital ID, and your goal is to find a way to get past the Beast so that you can continue on your journey.

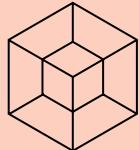
You've encountered beasts before, but the Beast of Digital ID is unlike any before. Many legends surround it. One of them states that there's a scale that lies in the center of the Beast's belly. According to legend, if you remove the scale, you defeat the Beast.

The legends tell of others who have found different ways to get past the Beast without defeating it outright. Some have learned to work with the Beast, slowly training it over time. Still others have managed to sneak past the Beast by finding other unguarded paths that allow them to continue on their journey.

You can fight the Beast, train the Beast, or seek another path around the Beast. Each option comes with its own tradeoffs, but you must ultimately find a way forward that makes sense given your capacity and resources.

You decide to momentarily retreat so that you can weigh your options and regroup.





Strategy 1: Fighting the Beast

Defeating the Beast means finding a way to remove the scale in the core of the Beast's belly that controls its powers. The Beast is well trained in protecting this sole vulnerability. To defeat it will mean being willing to be publicly and directly confrontational. Your goal won't be to compromise, but to win by dismantling the Beast and destroying its power. The process is not easy and will certainly require an arduous effort, but when the Beast is destroyed you'll have defeated it not just for yourself, but for all who travel the same path after you.

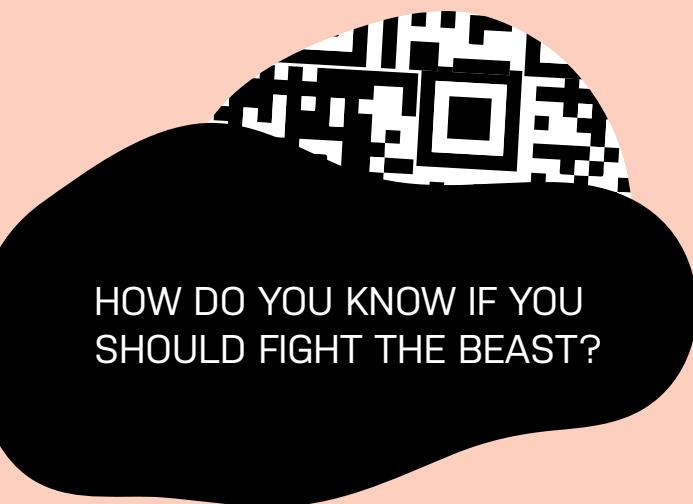
When it comes to digital ID systems, "fighting the Beast" usually looks like trying to prevent a digital ID system from being implemented in the first place. In the four countries that we've focused on, this type of battle has often taken place in the courts. In Uganda, a petition to the country's high court in March 2021 led the government to drop the requirement that residents be registered in the Ndaga Muntu Digital ID system in order to receive a Covid-19 vaccination.¹⁸ In Jamaica, litigation-based efforts forced the suspension of Jamaica's entire NIDS system. A constitutional court found that the system was intrusive in 2017, halting any governmental progress on it. As these examples show, the litigation approach has been successful.

But the Beast of Digital ID has multiple limbs. A part of it might be defeated, but other parts continue, allowing it to eventually return. This is exactly what happened in Jamaica, where the NIDS system was defeated in 2017 only to be reintroduced and ratified in 2021. Advocates in Tunisia dealt with the exact same phenomenon: a biometric ID card that they fought to defeat in 2018 was renewed and rolled out and expanded in 2020 to include an e-passport and an outline for a system that would store additional data points retrievable through a single ID number.¹⁹

Fighting the Beast means that you need to be realistic and clear in your aims. A win doesn't always have to strike at the heart of the system. Though it was a temporary solution, the litigation strategy in Jamaica did result in a blockage of the nation's digital ID system, and it built much more societal awareness around the NIDS system. Even temporary successes can carry a great impact.

18 Tsui and Perosa, *Digital IDs*, 2022.

19 Tsui and Perosa, *Digital IDs*, 2022.



HOW DO YOU KNOW IF YOU SHOULD FIGHT THE BEAST?

- **You know what drives the Beast.** It's crucial that you understand the many different factors that might push or influence the development of a digital ID system. For example, there might be private sector companies that are the real center of power of a system, rather than the government. If you don't already have this information you'll be at a distinct disadvantage.
- **You can be realistic and clear on long term goals.** Cutting off one limb of the Beast may slow it down temporarily, but this isn't the same as destroying its power. Fighting the Beast requires a clear sense of how one action will lead to another. Maybe you're just invested in changing one aspect of a digital ID system; maybe you want to stop the roll-out of a whole system. Either way, you need to know what your ultimate goal is in order to find your way there.
- **You can sustain the fight.** This work can be challenging, exhausting, and time-consuming. Make sure that you can sustain yourself for the long haul.

Fighting the Beast is a useful strategy when:

- **You can meet the resources of the system you're up against.** You can identify a weakness in a digital ID system and you can identify a strength of your own to overcome it. You don't need to have exactly the same types and numbers of resources as a government you're up against—you just have to know what your resources are and what you're capable of.
- **You want to take action in a way that's public and attention-grabbing.** Digital ID systems are often rolled out quickly without widespread public awareness. As the Jamaican legal cases that brought NIDS into the public eye showed, fighting the Beast can be a useful strategy for directing attention and public scrutiny towards a digital ID system.



Strategy 2

Training the Beast

Training the Beast requires getting into its mindset. You have to be able to understand how it works and what motivates it before you can get it to work with you. You also have to understand which different training methods are best.

When it comes to digital ID systems, "training the Beast" often looks like understanding and working alongside the governmental departments that are implementing the system. Digital ID systems are incredibly complex and oftentimes lack transparency. If you can convince governmental stakeholders to consider your perspective then you can attempt to transform the system from the inside out, making it more responsive to your community's needs.

Training the Beast has been the strategy of many policy and advocacy organizations in areas confronting the launch of digital ID systems. The Engine Room noted that in Indonesia, "the Arus Pelangi and Suara Kita organizations support registration efforts by collecting data from trans women who lack e-IDs and providing this information to the Dukcapil agency so that it can issue identity cards. By cooperating with the government in this way, the groups aim to guarantee trans people access to the system, while also shielding individuals from harassment and violence."²⁰ In this example, the Arus Pelangi and Suara Kita organizations realized that because their communities needed access to the e-KTP Digital ID system for essential services, the chief priority was finding a way to provide that access.

In other places, groups have voiced the desire to work with those implementing digital ID systems precisely because they were not consulted in the original design. In Uganda, the government's unwillingness to involve civil society in any aspect of the Ndaga Muntu program has been a significant barrier for residents and was likely responsible for low rates of participation in the early days of the system. This shows that training the Beast isn't always an option; its success depends on the willingness of the Beast to be trained.

20 Tsui and Perosa, *Digital IDs*, 2022.



HOW DO YOU KNOW IF TRAINING THE BEAST IS BEST?

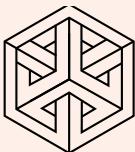
- **You have a way of assessing if change is taking place.** The challenge of the 'training the Beast' approach is ensuring that you accomplish your aims without bending to the desires of the Beast. The best way to tell if this is the case is by assessing if the Beast understands your needs and is changing its behavior in accordance with them. You'll want to look out for examples of direct change or opportunities that allow the Beast to share what it has learned. Without this certainty, you may find that the Beast is the one training you.
- **You have a clear and immediate access need.** The Arus Pelangi and Suara Kita organizations show how in moments of urgency, the most straightforward approach can be to find a liaison between the government and those that need to access services.

Training the Beast requires allies and indicators of success to help keep you on track.

You'll need to be able to clearly understand what you are looking for from the Beast, and to regularly assess if your demands are within reach. Training the Beast is the strategy of give and take.

Training the Beast makes sense when:

- **You have knowledge of how the Beast learns and what drives it to change.** You need to already understand something about the inner workings of a digital ID system in order to believe that working alongside the groups behind it can make a difference in your context.
- **You have or can build a relationship with the Beast.** This is a strategy that works best if you already have an existing connection within the system. Access is one of the largest reasons to employ this strategy.



Strategy 3

Seeking New Paths Around The Beast

You can directly confront the Beast, work with the Beast, or you can search for a completely different path that allows you to get what you want despite minimal interaction with the Beast. When you seek new paths, you are looking for loopholes and alternatives that allow you to chart a course free of gatekeepers.

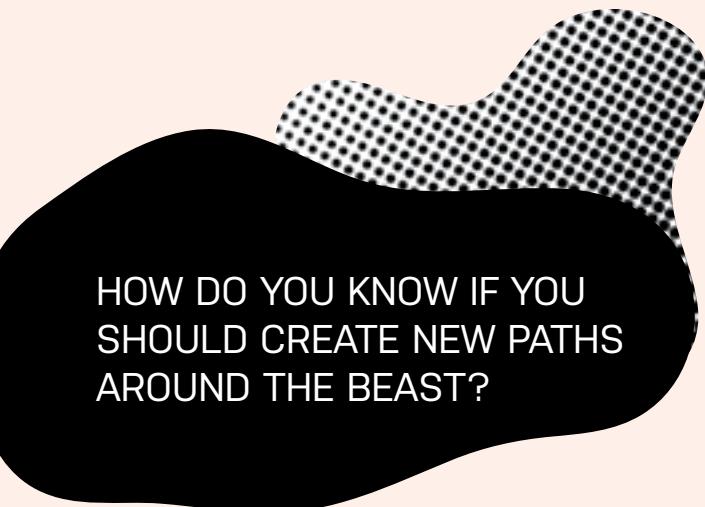
Seeking new paths is the strategy with perhaps the most freedom and variety in the forms it can take. It's also the strategy that holds the most uncertainty. It can manifest in small actions, like finding a way to share one form of identification with others in a system where each person is meant to have their own. This strategy relies on working collaboratively and collectively.

In Indonesia, indigenous individuals must present a religion statement from an organized group in order to be enrolled in the system. This presents a problem for indigenous individuals who do not belong to formalized organizations but are still required to present the form. Rather than appeal to the government, indigenous rights group MLKI stepped in to provide those statements. And MLKI doesn't stop here. The organization "is also engaged in capacity building, helping faith communities form their own official entities as a way of ensuring that their religious status registrations will be recognised, thus providing community members with access to identification."²¹

In both cases, MLKI creates new paths that are formed by learning what was required by the system, then finding alternative ways to satisfy those demands. Their actions show that seeking new paths doesn't mean being completely disconnected from Beast. It simply means keeping an eye on the loopholes that allow you to confront the Beast on your own terms.

This strategy suggests that one way to challenge a system is to neither fight it nor give in but instead to find ways around it that eventually drain its power. Perhaps the greatest strength of this strategy is the very thing that can make it difficult to assess: its openness. The fact that we don't know everything the environment around the Beast could hold means there is always an opportunity to discover an anomaly, a hack, or a gap to fill. Your biggest asset is your creativity.

21 Tsui and Perosa, *Digital IDs*, 2022.



HOW DO YOU KNOW IF YOU
SHOULD CREATE NEW PATHS
AROUND THE BEAST?

Seeking new paths makes sense when:

- You don't have the desire to fight or compromise with the Beast. Typically this is the case when you're working with a small group or when you have a need to move without public attention or fanfare. Because this is the strategy that minimizes the role of the Beast entirely, it is suited to those who have few existing connections with the Beast.
- You have the time and ability to put creative thought into the problem at hand. With this strategy, scanning for opportunities is just as important as being able to actually implement your plan. This is a strategy that requires being like water: you must adapt to every situation and keep moving.
- You can be discreet. This is a strategy that often involves moving in a more clandestine way. Unlike the previous two strategies, you're trying not to get the Beast's attention. Often this is better for smaller groups, or groups that have a high sense of internal cohesion and drive.

Choosing A Strategy

Often there isn't just one approach to confronting the Beast. It might be that different responses are called for at different times, or that a mixture of approaches is necessary. If you're working as part of a larger organization or field, different factions may each have their own strategy that make up a larger approach.

Perhaps the greatest skill that we can build—and a lesson that we can learn from our counterparts in Indonesia, Jamaica, Pakistan and Uganda—is our ability to assess the situations we find ourselves in and to have the flexibility and imagination to navigate ourselves, however slowly.

Below are a series of activities that you can use to guide yourself or your community in determining which strategy (or strategies) are best suited to determining your approach to responding to a national digital ID system.

Goals

Goals are meant to help you articulate what you want to achieve in your organization. They help you stay on track and give you a clear mission to return to when the process becomes messy or confusing.

Knowing clearly what your goals are is the first step to determining a strategy for moving forward.

If you don't have answers to the above questions, you may not yet be ready to carry out an organizing effort. Instead, go back to brainstorming. Regroup to get to a point where it's clear what exactly the problem is and what your needs are. Your goal is to be able to clearly identify what you are trying to accomplish and why.

What is/are the problem(s) your goals are solving?	
At the end of this organizing effort, what would you like to see accomplished? Write up to three things.	<ol style="list-style-type: none">1.2.3.
Who is your community? I.e., who are the groups whose situation will be improved by the achievement of your goals?	

Take a look at what you wrote above. Take note of the size of your goals. Are they clear and achievable? What else do you need to know about them?

Research

Research is understanding the basics of how the system that you are trying to change works. You need at least some sense of the system that you're navigating in order to determine a strategy towards it.

What would need to change in the existing digital ID system to accomplish your goal? Write up to three things.

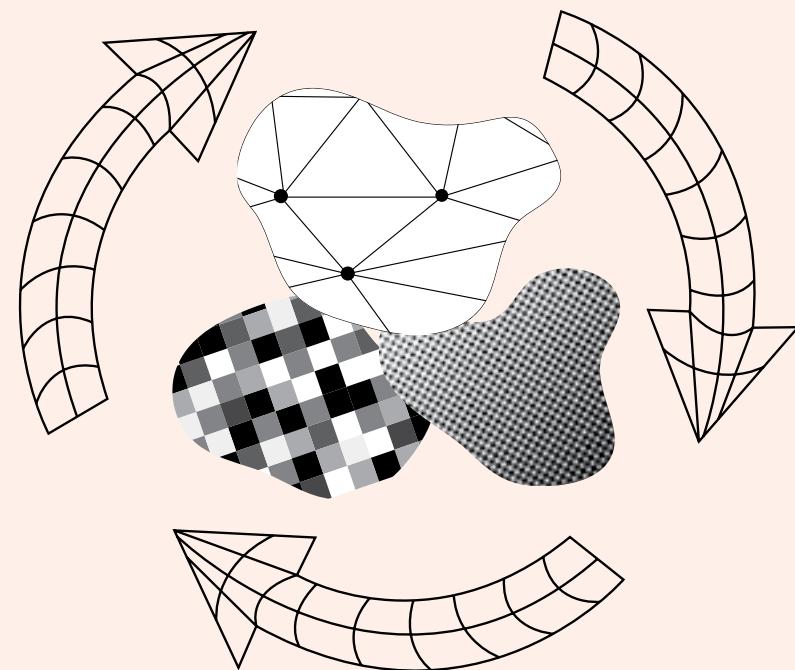
Who are the power brokers currently attached to the system?

Do you or could you have any connections to them?

What is the history of outside groups collaborating with or pushing against the existing system?

What has worked and hasn't worked?

Research will help you to learn about similar systems and tactics that folks in other places have used. If you find yourself struggling to answer some of these questions, flip back to the case studies section of this guide.



"The fact that we don't know everything the environment around the Beast could hold means there is always an opportunity to discover an anomaly, a hack, or a gap to fill. The only hindrance is your creativity."

Capacity

Once you know your goals, your next step is to assess your capacity. Your capacity is determined by your general availability and the resources at your disposal. These can come in many forms: they can be the energy and time you and your organization have, or an assessment of the number and type of people who can support you along the journey.

Use the below questions to assess what type of capacity you have when it comes to fighting a digital ID system.

<p>How much time do you have to dedicate to this new initiative?</p>	
<p>Who are your team members and allies? What groups and networks can you draw on?</p> <p>What skills, expertise, and resources do your team members and allies have?</p>	
<p>What projects are you already working on that can be connected to this effort?</p>	
<p>What knowledge do you hold that will influence this effort?</p>	
<p>What knowledge would you need to move forward with this effort? Where would you get it?</p>	

Based on your answers from the above section, you can begin to assess what makes sense given your own capacity, resources, and goals.

Go back to each of the strategies and look at the questions that help you determine if that strategy is for you.

Now read over your answers to the above questions. How do they line up? What patterns are emerging? Using the shortcuts below, identify what strategies line up with your specific situation.

Moving Forward: Support with Strategies

Now that you know your strategy, use the next sections to help you to move forward.

FIGHTING THE BEAST

When you have lots of resources, lots of people power, and/or want lots of attention.



Research

Research helps you understand how to get to where you want to be.

What are current laws or policies that support your effort?

What are current laws or policies that go against your effort?

What, if any court cases have made an impact in your area that align with your effort?

What strategies in your area have worked in shifting law or policies?

Team

The team is made up of allies or people you call on for support.

Who has worked on, or is currently working on, similar efforts in your area?

Who can support you with legal aid / representation?

What communities are impacted the most by your effort?

Who are community leaders you can call on for ideas and support?

Resources

Resources are the skills, materials, and assets that you have at your disposal.

What does this effort need to get off the ground?

What resources are readily available?

What needs to be financially accounted for in this effort?

How can this effort be funded?

TRAINING THE BEAST

When you are comfortable with collaborating and have direct access to the Beast. The Beast is open to discussion and compromise.

Goals

Goals are meant to help you articulate what you want to achieve.

At the end of this effort, what are three things you would like to see accomplished?

- 1.
- 2.
- 3.

What type of impact do you see those three things having in your community?

What evidence of impact are you looking to emerge in the future?

Research

Research helps you understand what you need to do based on how the system you are trying to change works.

What needs to happen to bring the goals above into action?

How does the system you are trying to train "learn"? In other words, what was required to bring previous changes to the system?

Team

The team is made up of allies or people you call on for support.

Who has or is currently working within the system you are trying to train?

Who are community leaders you can call on for ideas and support?

Who do you know that has been successful in a similar effort?

Strategy

Strategies are developed by assessing situations. They allow you to foresee how different situations are connected and can help you articulate how your actions can be reached through your goals.

Looking at your goals and research, what are three actions you can take to begin your training?

1.

2.

3.

How will you sustain this training?

What are signs or evidence you can look out for that will let you know your efforts are working?

FINDING NEW PATHS AROUND THE BEAST

When you have the ability to operate outside of mainstream structures. The Beast is not central to your strategizing.

Understanding the Problem

What is the core problem you are trying to address?

What are the consequences of this problem?

What are the conditions, institutions, and systems that reinforce this problem?

Making Connections

What are the commonalities that show up when unpacking the problem above?

What are the major differences you notice?

What are ways people are a part of the problem without even knowing it?

Generating Solutions

Where do you have control or agency over the problem?

What needs to happen for change to begin?

What do you believe can change in the short term?

What do you believe can change in the long term?

Designing the New

How are your solutions and/or ideas connected to others of the past?

How are your solutions and/or ideas different from what has been done before?

What needs to shift in order for your ideas to be adopted?

Bibliography

- Aizeki, Mizue, and Rashida Richardson. *Smart-City Digital ID Projects: Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions"*. Immigrant Defense Project, 2021.

Baker, Sara, and Zara Rahman. *Understanding the Lived Effects of Digital ID*. The Engine Room, 2020.

Community Justice Exchange. 2022. From *Data Criminalization to Prison Abolition*. <https://abolishdatacrim.org/en/report/full>.

Ho, Jennifer. "Imagining Our Futures: The Role of Technology in Social Justice Movements." *Public Interest Technology Party*. Lecture presented at the Public Interest Technology Party, 2019.

"NIDS Will Have Strongest Database Protection System in Jamaica, Says Green." Jamaica Observer. Accessed August 2, 2022. <https://www.jamaicaobserver.com/latest-news/nids-will-have-strongest-database-protection-system-in-jamaica-says-green>.

Patterson, Chris. "House Passes Nids Bill." Jamaica Information Service. Accessed May 27, 2022. <https://jis.gov.jm/house-passes-nids-bill-2>.

Rahman, Zara. 2018. "Digital ID: Why It Matters, and What We're Doing about It | the Engine Room." September 13, 2018. <https://www.theengineroom.org/digital-id-why-it-matters>.

Scott, James C. "State Projects of Legibility and Simplification." Essay. *In Seeing Like A State: How Certain Schemes to Improve the Human Condition Have Failed*, 65–66. New Haven: Yale University Press, 1998.

Srinivasan, Janaki, and Elisa Oreglia. "The Myths and Moral Economies of Digital ID and Mobile Money in India and Myanmar." *Engaging Science, Technology, and Society* 6 (2020): 215–36. <https://doi.org/10.17351/estss2020.276>.

"Sustainable Development Goals: United Nations Development Programme." UNDP. Accessed March 27, 2022. <https://www.undp.org/sustainable-development-goals>.

Tsui, Quito, and Teresa Perosa. Rep. *Digital IDs Rooted In Justice*. The Engine Room, 2022.

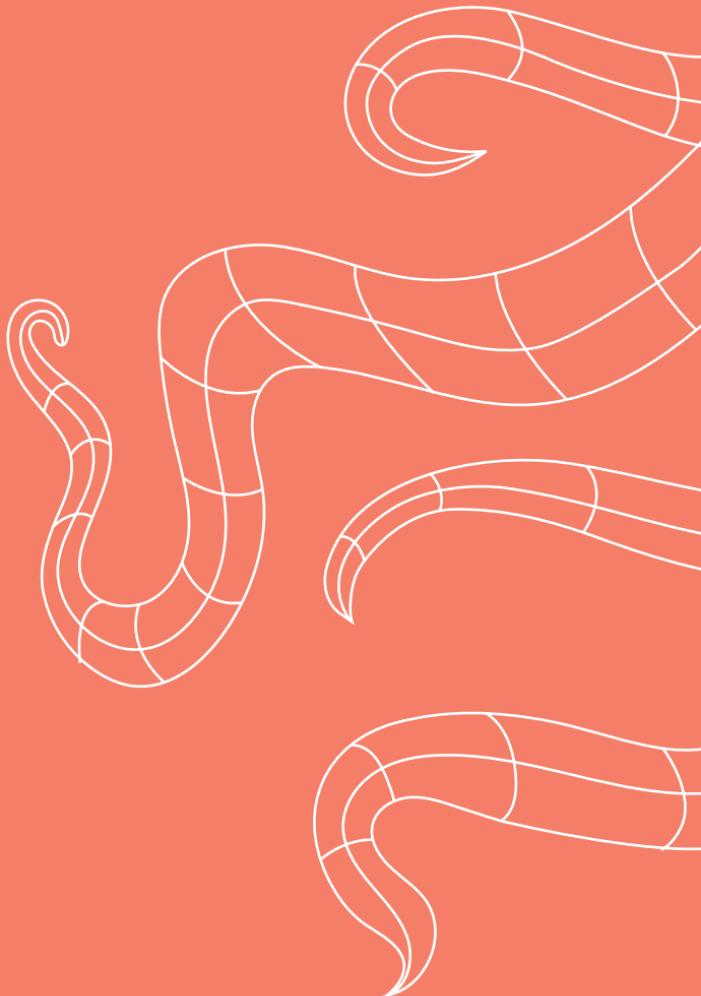
Victoria State Government. 2019. "Teach with Digital Technologies." Vic.gov.au. Education and Training. September 25, 2019. <https://www.education.vic.gov.au/school/teachers/teachingresources/digital/Pages/teach.aspx>.

Notes

Notes

Notes

Notes



\$10.00

ISBN 979-8-9866082-0-4

51000>



9 798986 608204