INSTRUCTIONS

This toolkit aims to help digital rights activists working on digital identification systems to navigate the complexities of the topic in an easier way, as well as to provide them with language that might help get them started in campaigning, advocating, educating, and mobilizing around digital ID systems. It is not a full, in-depth analysis of the landscape of digital ID systems or their potential risks and harms. It instead aims to provide a framework for thinking about digital ID systems and breaking them down to their distinct parts, particularly for non-experts.

The toolkit works as a "choose your own adventure" game where the player selects a **Persona** to start with and then navigates through the **System**, **Harm**, and **Mitigation** stages based on the person's circumstances.

Alternatively, play can begin from the System stage as a way to holistically analyze a specific digital ID system. For this, set aside the Persona deck and start by choosing the System cards that apply to the specific digital ID system you're studying.

FLIP THE CARD TO CONTINUE →

STAGES OF PLAY

System: These are characteristics a certain digital ID system might have. Persona cards call for System cards that have a particularly salient impact for that person's case, but characteristics not called for may also be present in the system. This set of cards focuses on the actual design and function of a digital ID system.

Harm: These are potential risks and harms that can arise from specific functions or processes that make up a system. In the same way as above, System cards call for the player to draw the most salient Harm cards, but the list is not exhaustive and other harms may also arise.

Mitigation: These are alternative approaches the ID system under study could adopt to help alleviate the potential harms caused by the identified system characteristics. We call them "mitigations" rather than "solutions" because most of the harms cannot be totally eliminated, and often several types of mitigation must be combined to be effective.

KNOW YOUR PLAYERS

Cards in the Persona deck describe people with fictional backgrounds based on real scenarios. They are not representative of all cases where harm might occur. Where a player wishes to better understand a specific situation, scenario, or system, they can use the blank card to create a custom Persona as a case study.

STARTER CARDS INCLUDE:

- LGBTQI+ person
- Person on the move
- Senior
- Person facing racial or ethnic discrimination
- Child
- Woman
- Person with disabilities
- Underprivileged person

BUILD YOUR OWN PERSONA:

To create a new Persona, start by asking questions about their circumstances and the system and society they live in. For example:

→ What is this person's gender and sexual orientation? Does this person's gender match the one they were assigned at birth? Does the system accept the recognition of this person's gender?

→ What is this person's racial and ethnic background? Are they part of the majority of the population in the place they live in? Is their ethnicity, religion, or race discriminated against or persecuted?

FLIP THE CARD TO CONTINUE →

KNOW YOUR PLAYERS

- → Does this person live in the place they're originally from? If not, how did they move (e.g. voluntarily, involuntarily, or under duress)? Do they have the same rights as someone that is originally from that place?
- → Does this person have any needs that are considered "special," such as a physical disability or mental health condition? Is there anything that might change the way they interact with the system? Does the system recognize and accommodate those needs?

These are just some examples of questions that you might ask when writing the story of your Persona. Giving them a name and a context helps you to understand their needs and potential risks they might face, and to then draw the appropriate cards from the System, Harm, and Mitigation decks.

To choose which System cards to draw, go through each and determine 1) whether the digital ID system you're analyzing contains this element (e.g., does it use biometrics? Is the database centralized?) and 2) whether this element puts the Persona you created at risk or potentially harms their human rights. Use the description on each System card to help determine if that is the case. If so, draw the card (including as many System cards as needed) and continue your gameplay by following the instructions on each System card.

PERSONA

Anya

LGBTQI+ PERSON

Anya is a trans nonbinary citizen of Iceland with a nonbinary gender marker on their passport. Anya needs to move to Italy for work, and Italy requires foreigners to carry identification at all times. The Italian ID card is intended for both digital and physical use, with biometric data printed on the card and stored on a contactless chip. The ID includes full name, place and date of birth, the holder's picture, and a fingerprint from each hand, and only allows for male or female gender markers. The card is not mandatory for Italian citizens but is the ID form most widely accepted in both the public and private sectors. The residency permit available to eligible foreigners is also digital and does not allow for nonbinary markers. If public security officers ask a person to identify themselves and are not satisfied by the answer, they may hold the person in custody until their identity is ascertained. The discrepancy between gender markers on Anya's Icelandic and Italian IDs as well as the forced adoption of a gender marker with which Anya does not identify both increase Anya's risk of being subjected to further investigation.

DRAW THE FOLLOWING SYSTEM CARDS:

Biometrics	Mandatory use
Centralized database	Exclusion by design


PERSONA
DIGITAL IDENTITY TOOLKIT

PERSONA

Luis

PERSON ON THE MOVE

Luis is a Venezuelan citizen with legal residence in the United States. His passport is expired and must be renewed before the five-year extension granted by the U.S. runs out. The Venezuelan system for issuing passports and national IDs is entirely online and is required for obtaining the needed appointment from the database's set list of embassies. For two months, this system has been completely down and nobody has been able to access the national registry database. There isn't a Venezuelan embassy or consulate in the U.S. that can issue Luis a new passport. To reach an embassy that can, Luis needs to travel to Mexico. However, Mexico will not accept his expired passport for entry and also requires a visa that can only be acquired with a valid passport. As a consequence, Luis will not be able to obtain a new passport, leaving him stranded in the U.S. where he will be overstaying his visa after the extension on his passport runs out.

DRAW THE FOLLOWING SYSTEM CARDS:

- Biometrics
- Mandatory use
- Lack of accessibility
- Opaqueness


PERSONA
DIGITAL IDENTITY TOOLKIT

PERSONA

Birhanu

PERSON FACING RACIAL OR ETHNIC DISCRIMINATION

Birhanu is a Tigrayan living in Addis Ababa, Ethiopia. During the civil war, ethnic origin was used to round up people and accuse them of being rebels, a situation that particularly affected male adults of Tigrayan origin. Following the ceasefire, the Ethiopian government is implementing a nationwide biometric digital ID system backed by the World Bank, aiming to register all eligible adults of its population of 119 million by the end of 2025. Ethiopia doesn't have a proper data protection law, though it does have scattered legislative norms requiring some standards of care for data collection and processing.

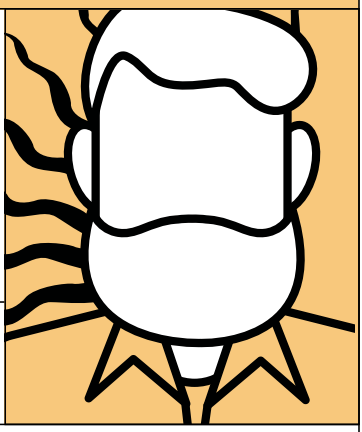
DRAW THE FOLLOWING SYSTEM CARDS:

- Lack of strong data protection framework
- Lack of human rights impact assessments
- Biometrics
- Mandatory use


PERSONA
DIGITAL IDENTITY TOOLKIT

PERSONA

Patricio



SENIOR

Patricio is a 74-year-old Chilean man who has worked his entire life as a bricklayer, a profession that has worn down the ridges of his fingerprints to the point of making them very difficult for machines to recognize. Every time Patricio needs to go through a fingerprint scanner, it is a long and tiresome process that often feels humiliating. Patricio is also unfamiliar with technology, which makes these procedures uncomfortable. Patricio often must go through this process to access public services or when he needs healthcare, and he has been repeatedly denied from seeing a doctor because his identity could not be verified through his fingerprints.

DRAW THE FOLLOWING SYSTEM CARDS:

Biometrics	Mandatory use
Lack of accessibility	Centralized database


PERSONA
DIGITAL IDENTITY TOOLKIT

PERSONA

Janine

CHILD

Janine is a seven-year-old migrant seeking asylum in the UK. The UK requires children under five years old to attend a biometrics appointment to take digital photos as part of the entry clearance application, and those over five must also provide their fingerprints. Children under the age of 13 typically cannot validly consent to using services such as social media apps, and regulations like the GDPR require children between 13 and 16 years to have verifiable parental consent for the processing of their data. However, many academics agree that the collection of biometric data requires a higher standard, and valid consent is likely not possible from either the child or parent where bodily autonomy is in question.

DRAW THE FOLLOWING SYSTEM CARDS:

Biometrics	Mandatory use	Exclusion by design
Centralized database	Lack of human rights impact assessments	


PERSONA
DIGITAL IDENTITY TOOLKIT

PERSONA

Anousheh

WOMAN

Anousheh is a woman living in Afghanistan. The Afghan Identity Card, also known as Tazkira, is a document that serves as a proof of identity, residency, and nationality for Afghans. In its digital form, the E-Tazkira contains information such as the person's name, their personal ID number, and other basic information, as well as biometric information such as iris scans, fingerprints, photographs, and other personal information like their occupation, their home addresses, and the names of their relatives. However, across Afghanistan, 56% of women do not have an E-Tazkira ID card. Since they are denied permission to obtain the card themselves, they need the support of their male family members to obtain them, and, in many places, it is considered shameful for female family members to obtain these documents. This, in consequence, means women are routinely denied basic human rights.

DRAW THE FOLLOWING SYSTEM CARDS:

Biometrics	Mandatory use	No remedy and redress
Centralized database	Exclusion by design	Lack of accessibility
Lack of strong data protection framework	Lack of human rights impact assessments	Opaqueness


PERSONA
DIGITAL IDENTITY TOOLKIT

PERSONA

Farhad

PERSON WITH DISABILITIES

Farhad is an Indian man living with neurological disabilities. In order for Farhad to be enrolled in Aadhaar, he needed to sit still for the photograph and have his iris scanned, both processes that triggered his neurodivergence and made the entire process stressful and traumatic for him. As the people handling the process were not always patient enough to accommodate Farhad's needs, it took him three tries in three different centers to be able to enroll. After many attempts by civil society, the government has adopted changes to Aadhaar that makes it more accessible to physically disabled people, but these changes do not include any accommodations for neurological disabilities.

DRAW THE FOLLOWING SYSTEM CARDS:

Biometrics	Mandatory use	No remedy and redress
Centralized database	Lack of accessibility	Opaqueness


PERSONA
DIGITAL IDENTITY TOOLKIT

PERSONA

Susana

UNDERPRIVILEGED PERSON

Susana's country's ID system uses Gemalto's mobile ID Smart App, which is required for most transactions. Susana is a 68-year-old woman who is unfamiliar with technology and who owns an old smartphone and can't afford a new one. The app that Gemalto built and sold to the government for this digital ID system doesn't work on earlier operating systems, and therefore Susana cannot use it on her phone. The app also requires the use of biometrics, which makes it more difficult for Susana to get help from her daughters to access the system from their phones.

DRAW THE FOLLOWING SYSTEM CARDS:

Biometrics	Mandatory use	Lack of accessibility
Centralized database	Lack of human rights impact assessments	Lack of strong data protection framework


PERSONA
DIGITAL IDENTITY TOOLKIT

BUILD YOUR OWN PERSONA

NAME

?

DESCRIPTION

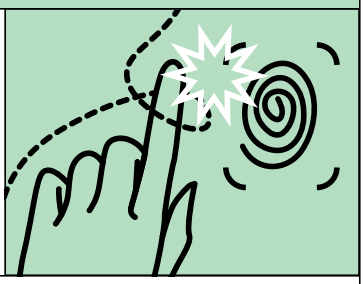
STORY

DRAW THE FOLLOWING SYSTEM CARDS:


PERSONA
DIGITAL IDENTITY TOOLKIT

SYSTEM

Biometrics



Biometric data is information about personal characteristics that are generally unique to an individual. These can be physical or behavioral. Physical biometric data may include, for example, one's facial features, fingerprints, or iris patterns, while behavioral biometric data may include attributes such as gait, signature, or voice patterns.

Most often, biometrics are used in digital ID systems as the primary mechanism for verifying a person's legal identity. This can be dangerous, as most often an individual cannot change their biometric data, making it extremely sensitive and difficult to remedy in the case of a data breach. It can also be ineffective, since the identifying characteristics are not always immutable. For instance, a person's gait, voice timbre, or face shape may change as they age, or a trans person may change their attributes typically associated with gender.

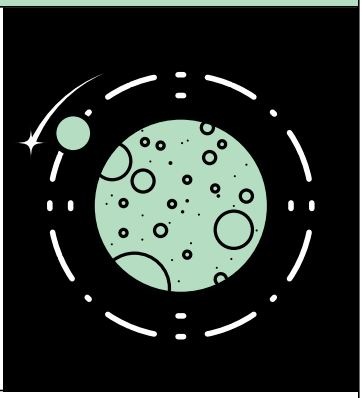
USING BIOMETRICS CAN LEAD TO:

- Surveillance
- Discrimination
- Dehumanization
- Artificial constraints on autonomy
- Data insecurity


SYSTEM
DIGITAL IDENTIFY TOOLKIT

SYSTEM

Centralized database



Digital ID systems often use a centralized database to store many different types of information about an individual. This can go beyond basic information from an ID card to also record a person's interactions with different government agencies, service providers, and private companies. Consolidating large amounts of non-anonymized personal information creates a high-value target for hackers and increases the severity of data breaches, leading to harassment, identity theft, and data loss. This also means a single point of failure for the overall system should the database stop working. Multiple authorities typically have access to the centralized database, increasing the temptation for many actors to abuse the available data for surveillance or other purposes.

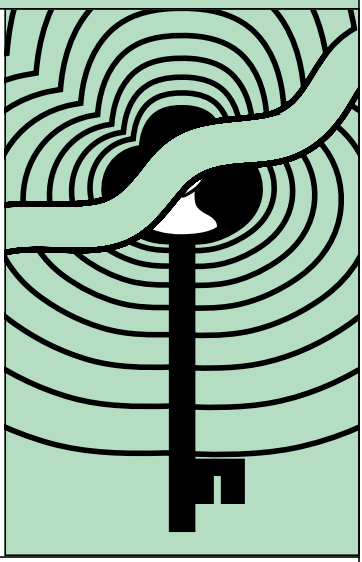
A CENTRALIZED DATABASE CAN LEAD TO:

- Surveillance
- Data insecurity
- Broken infrastructure


SYSTEM
DIGITAL IDENTIFY TOOLKIT

SYSTEM

Lack of strong data protection framework



A proper data protection framework is used to help guarantee that people have control and agency over their personal information, and that public and private organizations collecting personal data are held accountable for its protection and proper use. This framework should include the principles of consent, lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. Without such a framework in place, a digital ID system is likely to be overreaching in its initial design and implementation, and also to proliferate over time well beyond its initial purpose, exposing people to further risk.

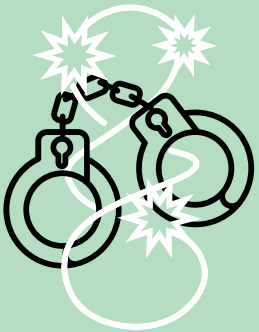
A MISSING OR WEAK DATA PROTECTION FRAMEWORK CAN LEAD TO:

- Surveillance
- Discrimination
- Dehumanization
- Artificial constraints on autonomy
- Data insecurity


SYSTEM
DIGITAL IDENTIFY TOOLKIT

SYSTEM

Mandatory use



A digital ID system is mandatory when it becomes, by law or by practice, the only way for a person to provide proof of their legal identity. In many so-called "foundational" ID systems, the digital ID becomes the only trusted source of basic identity information between a person and the government or authority that requires the authentication of that identity, thus replacing any previously existing mechanisms to prove someone's identity, such as paper-based identification, if they existed before. For a digital ID system to be non-mandatory, there must always be analog alternatives in place.

While all mandatory digital systems are dangerous, there is an additional layer of human rights harm when a system mandates collection of biometric data, since this represents the forced digitization of the human body and loss of bodily autonomy.

MANDATORY USE CAN LEAD TO:

Surveillance	Discrimination	Dehumanization
Artificial constraints on autonomy	Data insecurity	No access to public services


SYSTEM
DIGITAL IDENTIFY TOOLKIT

Exclusion by design

A digital ID system introduces exclusion by design when the way the system operates, how it is used, or the types of behaviors it encourages result in certain individuals or communities being unable to safely and effectively participate in that system. Sometimes systems are explicitly designed to exclude (e.g. a system that is meant to recognize, surveil, or prosecute a certain category of people, such as ethnic populations, immigrants or refugees, or women), while other systems exclude as an unintended or negligent consequence of poor design (e.g. a system that disallows the election of gender identity).

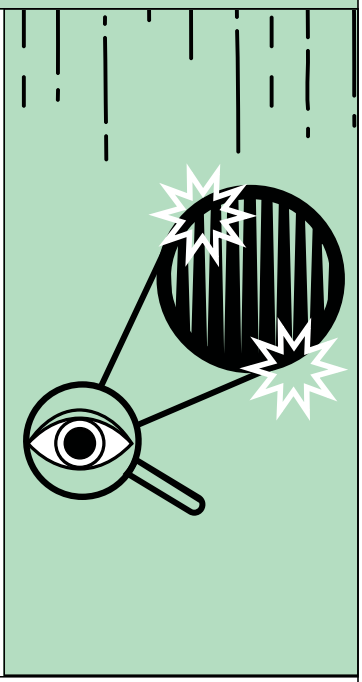
EXCLUSION BY DESIGN CAN LEAD TO:

- Discrimination
- Dehumanization
- No access to public services
- Artificial constraints on autonomy


SYSTEM
DIGITAL IDENTIFY TOOLKIT

SYSTEM

Lack of human rights impact assessments



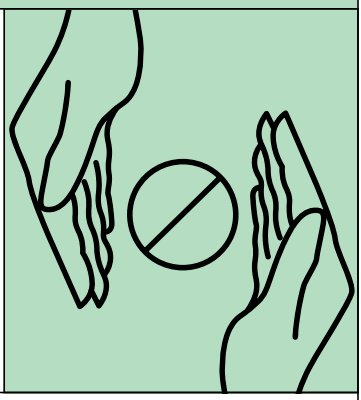
Before implementing any digital ID system, all relevant stakeholders, including government, companies, and international financial institutions, should undergo thorough, independent human rights impact and data protection impact assessments to identify, assess, and address any potential harms the system may cause or exacerbate. In all cases, such assessments should be undertaken in close collaboration with a diverse cross-section of civil society and at-risk communities. Failing to evaluate potential human rights risks early in the design and development process, and to maintain those assessments throughout the system's life cycle, will very likely result in serious harms that are difficult to reverse later on.

FAILURE TO CONDUCT HUMAN RIGHTS IMPACT ASSESSMENTS CAN LEAD TO:

Surveillance	Discrimination	Dehumanization
Artificial constraints on autonomy	Data insecurity	Broken infrastructure


SYSTEM
DIGITAL IDENTIFY TOOLKIT

No remedy and redress



Every digital ID system should include effective mechanisms for remedying violations of international human rights and international humanitarian law, including the right to equal and effective access to justice; adequate, effective, and prompt reparation for harms suffered; and access to relevant information concerning violations and reparation mechanisms. Not having access to effective judicial remedy – including reparation, restitution, compensation, satisfaction, rehabilitation, and guarantees of non-repetition, as applicable – perpetuates human rights violations and goes against the international legal principles of accountability, justice, and the rule of law.

Even the most highly safeguarded systems will see human rights issues arise, and in all cases, where victims are not able to hold perpetrators of human rights violations to account, they are more likely to continue.

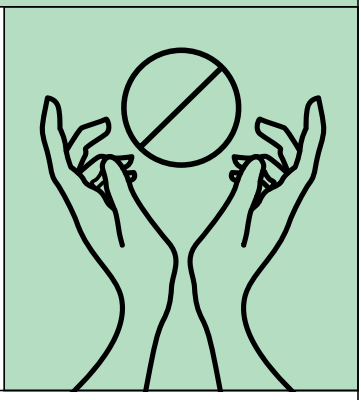
WITHOUT REMEDY AND REDRESS, A SYSTEM IS MORE LIKELY TO LEAD TO:

- Surveillance
- Discrimination
- Dehumanization
- Artificial constraints on autonomy
- Data insecurity


SYSTEM
DIGITAL IDENTIFY TOOLKIT

SYSTEM

Lack of accessibility



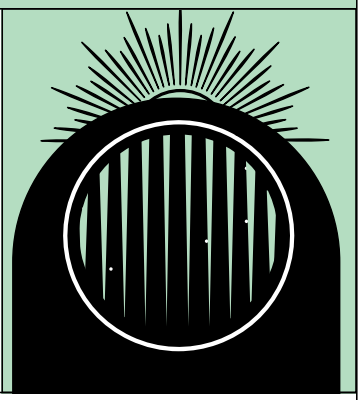
Digital ID systems, particularly those using biometric recognition, are not always accessible for people with disabilities, older people, or people whose fingerprints or other biometric indicators have been eroded or deformed, because they often face complications both at the time of collection and at the time of authentication. Likewise, the collection of biometric measurements can be an intrusive procedure to people's bodies, which can severely impact people who have intellectual or developmental disabilities, as well as any disorders that affect how the brain processes or interprets information from the senses.

WHEN A DIGITAL ID SYSTEM IS NOT ACCESSIBLE, IT CAN LEAD TO:

- Surveillance
- Discrimination
- Dehumanization
- Artificial constraints on autonomy
- Data insecurity


SYSTEM
DIGITAL IDENTIFY TOOLKIT

Opaqueness



Digital ID systems deployed in opaque and unaccountable ways can harm individuals and exacerbate pre-existing biases. All opaque systems that impact people's access to human rights have the potential to be invasive, biased, unfair, and manipulative, and to pose threats to data privacy and other democratic values like autonomy, fairness, and transparency.

Systems that are designed and developed behind closed doors, with little to no public consultation or meaningful engagement from civil society, are opaque by default. Often, the procurement of these systems is also opaque, with no available information on technical standards and technologies that are being used, and even without the procurement process itself being open.

OPAQUE DIGITAL ID SYSTEMS CAN LEAD TO:

Surveillance	Discrimination	Dehumanization
Artificial constraints on autonomy	Data insecurity	Broken infrastructure


SYSTEM
DIGITAL IDENTIFY TOOLKIT

SYSTEM

Unduly obtained consent

When ID systems enroll people under conditions that do not allow for meaningful informed consent, then that consent is invalid and therefore void. This happens, for instance, when collecting biometric data from children, but also when enrolling people who do not have access to alternatives that do not imply a significant harm or expense, such as refugees or impoverished people who require a digital ID to access subsidies.

OPAQUE DIGITAL ID SYSTEMS CAN LEAD TO:

- Surveillance
- Discrimination
- Dehumanization
- Artificial constraints on autonomy
- Data insecurity


SYSTEM
DIGITAL IDENTIFY TOOLKIT

Surveillance

Certain technologies (e.g. biometric recognition) used to identify individuals and collect their personal data – as well as those systems' legal and technical infrastructure – facilitate overreaching surveillance. Practices such as categorization of bodies, cataloging of ethnicities, or tracking of people's movements all bring consequences for freedom of speech, privacy, and ultimately people's autonomy, damaging the fabric of democratic society.

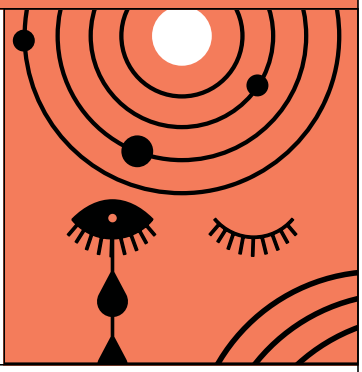
Surveillance linked to someone's legal identity – and therefore their relationship with a state, their standing in society, and their ability to gain access to welfare, healthcare, and other basic services – is highly invasive, undermines their ability to fully and meaningfully engage in society without fear of repercussions, and deepens existing discrimination and inequities.

POSSIBLE MITIGATIONS TO PREVENT OVERREACHING SURVEILLANCE INCLUDE:

- Opt-out / opt-in mechanisms
- Access to public services without identification
- Data protection framework
- Limited biometrics
- Data minimization


HARM
DIGITAL IDENTITY TOOLKIT

Discrimination



Through every stage of their design, development, and implementation, digital ID systems can easily amplify existing forms of discrimination or introduce new ones. When a system does not properly account for the needs of a specific community, they are likely to be left behind – cut off from essential services, forced to overcome additional barriers, and confronted with difficult tradeoffs between being treated with dignity and being granted access to their rights. At its worst, discriminatory functions are built into the system intentionally, putting people at even greater risk of serious harm, ranging from targeted surveillance, detention, and deportation to denial of services, forced misgendering, and more.

POSSIBLE MITIGATIONS TO PREVENT DISCRIMINATION INCLUDE:

- Safeguards and accountability
- Access to public services without identification
- Data minimization
- Transparency


HARM
DIGITAL IDENTITY TOOLKIT

Dehumanization

The use of certain technologies that force people into the digitization of their bodies and the storage of data about them in places over which they cannot exercise full control – particularly in places where these systems are used for the distribution of public assistance or welfare – can be an attack on autonomy, human dignity, and bodily integrity, treating data about the body as something that can and must be traded to access other fundamental rights.

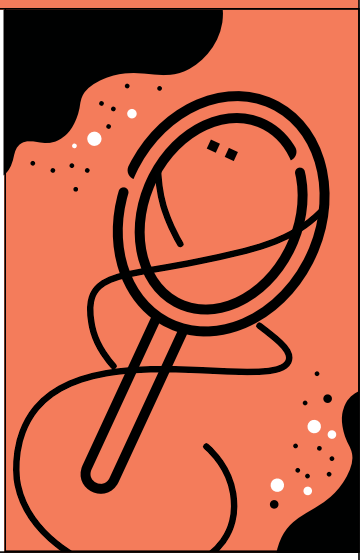
POSSIBLE MITIGATIONS TO PREVENT DEHUMANIZATION INCLUDE:

- Limited biometrics
- Remedy and redress
- Data minimization
- Safeguards and accountability
- Opt-in / opt-out mechanisms
- Data protection framework
- Access to public services without identification


HARM
DIGITAL IDENTITY TOOLKIT

HARM

Artificial constraints on autonomy



Digital ID systems often require individuals to misidentify themselves in order to access a certain place, service, or action. For instance, someone who identifies as nonbinary might be required by the system to identify either as male or female. By forcing a choice between maintaining one's full identity or accessing basic rights and services, the system undermines the person's ability to navigate the world with autonomy and dignity. These artificial constraints marginalize people, deter their participation in society, and further classify them as "invalid." They also introduce collection of sensitive data that is typically not necessary for the system to function properly.

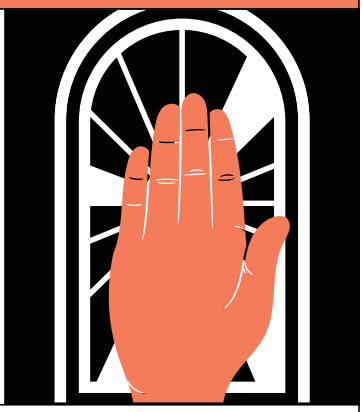
POSSIBLE MITIGATIONS TO AVOID ARTIFICIAL CONSTRAINTS ON AUTONOMY INCLUDE:

- Limited biometrics
- Remedy and redress
- Data minimization
- Safeguards and accountability
- Opt-in / opt-out mechanisms
- Access to public services without identification
- Transparency


HARM
DIGITAL IDENTITY TOOLKIT

HARM

No access to public services



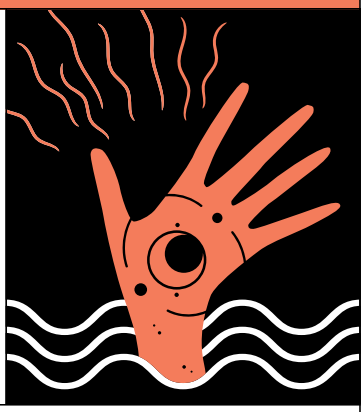
Digital ID systems – often deployed by governments with the stated purpose of improving access to public services, especially those linked to welfare and financial aid – can introduce barriers to access for the people most in need. A person may be cut off from accessing services through the digital system because they lack meaningful access to technology, because they have specific attributes or experiences that prevent them from easily interacting with the system, or because the system exacerbates existing models of exclusion or disenfranchisement. The immediate and compounding harms of being denied access to basic public services like water, housing, healthcare, or education are almost beyond measure, pushing vulnerable people deeper into the margins and making it impossible for them to climb out.

POSSIBLE MITIGATIONS TO PREVENT LOSS OF ACCESS INCLUDE:

- Access to public services without identification
- Opt-in / opt-out mechanisms
- Data minimization


HARM
DIGITAL IDENTITY TOOLKIT

Data insecurity



Digital ID system databases – particularly when centralized – can pose one of the biggest dangers possible to people's privacy. These systems often assemble excessively comprehensive profiles of personal data, with each additional data point adding another layer of risk. Around the world, leaks and hacks of these databases have led to missing data, stolen identities, fraud, and many other types of physical and mental harm that fall entirely out of affected people's control. Matters are only made worse where there is no meaningful legal framework for data protection, leaving people with limited options to recover their losses.

POSSIBLE MITIGATIONS FOR DATA INSECURITY INCLUDE:

- Limited biometrics
- Remedy and redress
- Data minimization
- Safeguards and accountability
- Opt-in / opt-out mechanisms
- Open-source technology
- Decentralized databases
- Data protection framework


HARM
DIGITAL IDENTITY TOOLKIT

Broken infrastructure

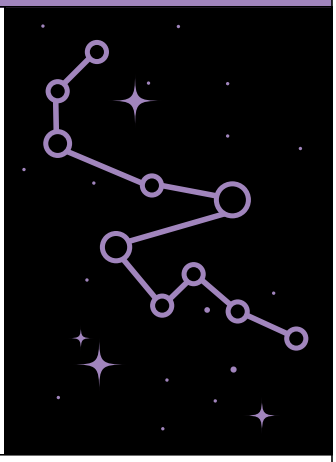
When designing a digital ID system, it is necessary to consider not only its possible consequences and goals, as well as the needs for its development and rollout, but also how it will be maintained over time – an aspect proponents of these systems often overlook. This oversight is especially damaging in countries that don't have the underlying resources to keep a consuming system properly working, leading to breakdowns in the system's infrastructure and disruptions to access. This can make the situation worse than before the system was installed, especially once other processes have adapted to identification working digitally.

POSSIBLE MITIGATIONS FOR BROKEN INFRASTRUCTURE INCLUDE:

- Limited biometrics
- Remedy and redress
- Data minimization
- Safeguards and accountability
- Opt-in / opt-out mechanisms
- Open-source technology
- Decentralized databases
- Access to public services without identification
- Data protection framework
- Transparency


HARM
DIGITAL IDENTITY TOOLKIT

Decentralized databases

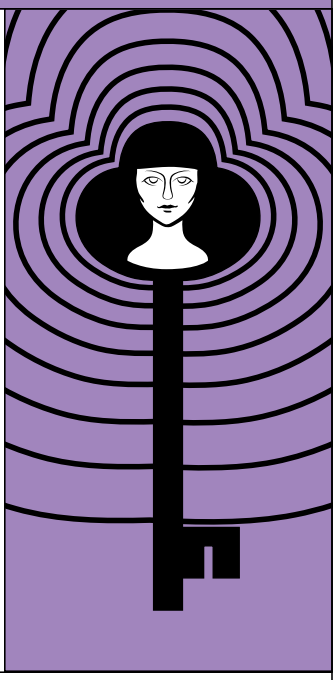


Governments tend to prefer a centralized approach that involves a unique identifier number that can track an individual across different services, since such systems provide governments much more information about their populations, leading to heightened risk of surveillance, discrimination, and data insecurity. Decentralized databases can take many different approaches and many different technological structures, and not all of them are ideal. But when designed carefully – considering accessibility, technical viability, service delivery, and other key factors – a decentralized approach can grant people greater access to and control over their data and provide a stronger framework for managing data sharing and preventing leaks.

MITIGATION

DIGITAL IDENTITY TOOLKIT

Data protection framework

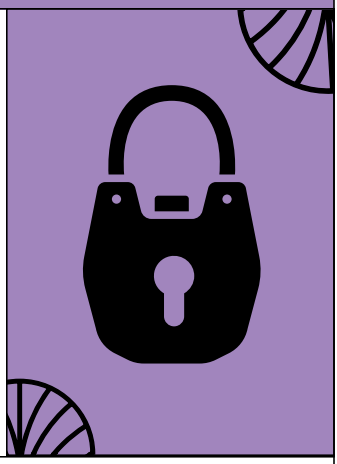


To ensure human rights are protected, governments should have a strong, fully operational data protection framework in place before adopting any kind of digital ID system. Many countries still don't have such a framework, and thus do not have even the most basic protections required for building a rights-respecting digital ID system. The minimum data protection framework necessary would include, at the very least, eight principles: consent; lawfulness, fairness, and transparency; limitation of purpose; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

MITIGATION

DIGITAL IDENTITY TOOLKIT

Limited biometrics

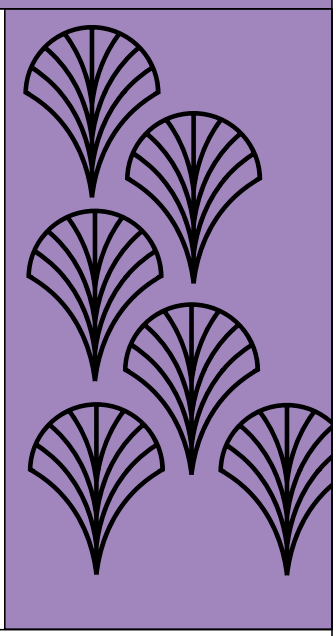


Although it has become normalized, the collection of biometric information is a very delicate process that can affect a wide range of fundamental rights. Collecting biometric information is rarely justified, and biometrics are not necessary or appropriate in all contexts. For example, in certain scenarios, multi-modal biometrics might give individuals more flexibility to choose which data they want to provide, but more often they deepen problems by requiring several types of biometric data simultaneously. In any circumstance, individuals who cannot provide meaningful consent over their bodies, such as children, should never be required to provide biometric information. Biometric data should also always be safely discarded as soon as the biometric templates are created in a way that does not allow the data to be restored to its original form.

MITIGATION

DIGITAL IDENTITY TOOLKIT

Safeguards and accountability

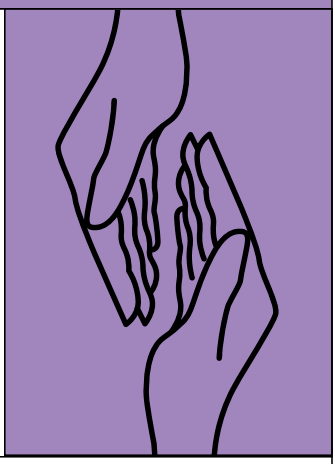


Before a digital ID system is rolled out, the administering government should have clear safeguards in place to protect the confidentiality, integrity, and availability of the system and its data. These safeguards should be comprehensive, integrating a wide range of different measures – including, for example, security protocols for data, devices, and physical structures and clear limits to staff privileges and access to data. Safeguards should also protect against errors like duplicate identities or repeated identifiers, alterations or other unauthorized changes to the data, and data misuse. In parallel, strong accountability mechanisms must hold system administrators responsible when issues arise and lead to corrections to avoid the same problems going forward. Such processes are essential for protecting individuals' fundamental rights as they engage with the system, and for upholding the trust necessary to allow the digital ID system to effectively function.

MITIGATION

DIGITAL IDENTITY TOOLKIT

Remedy and redress

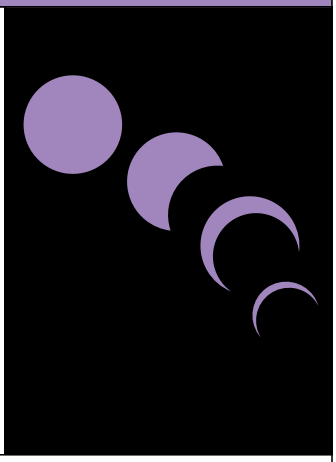


When a person's human rights have been violated, they are entitled to remedy – meaning access to justice, some form of reparation or redress (such as monetary compensation), and rehabilitation. Likewise, all digital ID systems should include pathways for addressing any human rights harms they may cause from the outset. Clear, accessible mechanisms for remedy and redress empower individuals and communities to exercise control over the system and hold its administrators accountable, as well as to obtain compensation for damages they have suffered. In addition to a clear legal foundation for the redress mechanism, people also need to have easy access to information regarding how to present and follow up on a request, and authorities must provide a timely, just response.

MITIGATION

DIGITAL IDENTITY TOOLKIT

Data minimization

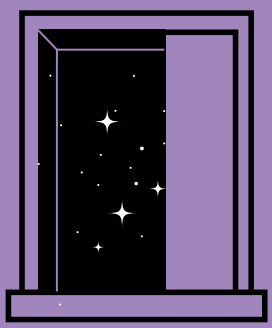


One of the most fundamental principles of data protection is data minimization – which means a system should only collect and retain the minimum amount of data necessary to perform its intended function. Despite this, digital ID systems tend to encompass a large number of data points, such as someone's address, gender/sex markers, citizenship status, ethnicity, etc. In most cases, governments claim many of the data points collected by digital ID systems that aren't strictly necessary for verifying someone's identity are still necessary for statistical purposes. However, this type of data should be collected by means of a population census and should be anonymized and safeguarded in ways that prevent any data from being traced back to a specific respondent. Most of this information is not needed for any specific interaction with the state, or can be provided on an as-needed basis, and should not be incorporated into a digital ID system.

MITIGATION

DIGITAL IDENTITY TOOLKIT

Opt-in/opt-out mechanisms



Individuals can only provide real consent to the collection and processing of their data in a digital ID system when they have a feasible alternative available and refusing to participate in the system is a viable option. There should always be easy and accessible mechanisms to either opt in or opt out of a specific system or parts of it. In particular, every digital ID system should have one or several analog alternatives available. Digital ID should never be understood as a synonym of legal identity, but rather only as a way of proving the relationship between a person and a state or similar institution. The fundamental right to a legal identity should always allow for a diversity of ways to prove it, both through analog and digital means, and any identity system should always presume the good faith of people as well as their being entitled to fundamental human rights even in absence of proof.

MITIGATION

DIGITAL IDENTITY TOOLKIT

Open-source technology

Open-source technology can often be an alternative when attempting to avoid technological lock-in by specific vendors. A system being open source can help make it easier to reuse and adapt, more resilient, and even safer if it can be thoroughly audited by independent security researchers. However, it doesn't by itself solve many of the potential problems, and can sometimes create new issues, particularly if it isn't accompanied by the necessary training and nurturing of local expertise capable of handling the system.

MITIGATION

DIGITAL IDENTITY TOOLKIT

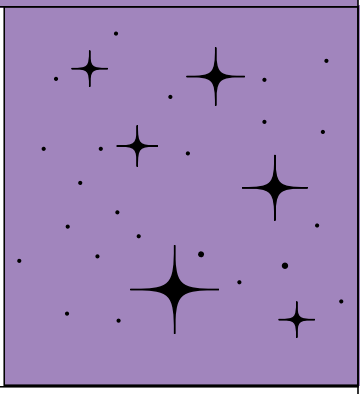
Access to public services without identification

In many cases, governments that have invested in the development of a digital ID system continuously seek out opportunities to expand its use, even to interactions that should not require any type of identification (e.g. simple commercial transactions, access to public WiFi networks provided by the state, or public healthcare services). When designing a system, there should be careful consideration regarding whether the authentication of a person should be required to allow them access to a specific service. Many services, both public and private, can be provided without knowing a person's identity, and therefore should be made available as anonymously as possible. In other scenarios, such as healthcare (particularly reproductive healthcare), the characteristics of the information required are such that it should only be required by the provider itself and not stored in a centralized database along with other types of personal information.

MITIGATION

DIGITAL IDENTITY TOOLKIT

Transparency



To build a well-functioning and trustworthy digital ID system, a government must be transparent and engaged with the people and communities the system is likely to impact. Transparency in the process should start the minute a government is even considering replacing or implementing a digital ID system and continue every step of the way, particularly during the procurement process and after implementation. Governments and other stakeholders cannot achieve transparency by merely sharing information about decisions they've already made, publicly promoting the system, or holding cursory "consultations" with civil society that will not meaningfully shape the process.

MITIGATION

DIGITAL IDENTITY TOOLKIT