HUMAN RIGHTS
FOR DIGITAL IDENTITY
COALITION

Common Position Statement on Mandatory Digital IDs

Table of Contents

HUMAN RIGHTS
FOR DIGITAL IDENTITY
COALITION

About the Human Rights for Digital Identity (HR4ID) Coalition

We are a transnational community of civil society organizations, researchers, and advocates dedicated to advancing equity, justice, and human rights in digital identity systems. As state-driven digital transformation accelerates—often without community consultation—our network provides a platform for solidarity, research, advocacy, and collective action to resist and reshape digital ID programs that undermine rights and dignity.

To learn more, please contact us at admin@hr4id.org.

Summary

As public institutions increasingly turn to digital ID to mediate online and offline interactions, a critical question is: under what circumstances, if any, should digital ID be mandatory? To address this question, the Human Rights for Digital Identity (HR4ID) Coalition has developed **four principles that summarize our core concerns and recommendations**, which are:

1. Mandatory digital ID requirements negatively impact human rights and human life, particularly for those who are marginalized or vulnerable.
2. Public institutions should not require *mandatory enrollment* in a digital ID system.
3. Public institutions should not require *mandatory use* of elements of the digital ID system to access public services or privately provided public services.
4. In contexts where digital ID systems already exist or are in development, the State has an obligation to guarantee that equal, adequate, and accessible alternatives are available–including non-digital options–for those who are not enrolled or who do not use the digital ID.

Our recommendations are rooted in our understanding that mandatory digital ID requirements impact many aspects of human life, particularly for those who are already marginalized or vulnerable. This includes requirements to *enroll* in a specific digital ID system or to *use* a specific digital ID system in order to access services, processes, or online and offline spaces. It includes systems that are mandatory *in law*, as well as systems that may appear voluntary but are mandatory *in fact*. For those who do not comply with such requirements, the negative consequences can include exclusion from public services, as well as other forms of stigmatization and discrimination, preventing people from enjoying fundamental human rights. Even for those who do comply, being included in the system can lead to harm, especially due to the omnipresent risk of function creep. This can lead to violations of privacy and data protection, targeted mistreatment, and the creation of interoperable data systems that can be used to surveil, coerce, discriminate, and persecute.

Public institutions have obligations to respect, protect, and fulfill human rights—and also hold significant power to decide which individuals and communities get to enjoy these rights. Therefore, it is vital that these institutions refrain from imposing or facilitating requirements that may lead to harm. Moreover, public institutions have a positive obligation to take action to improve equal treatment and enjoyment of human rights. To avoid the violations of rights that may result from requiring any single form of digital ID system in order to access services, States should take steps to ensure that equal, adequate and accessible alternatives remain available.

Digital ID systems come in many forms, and the political, legal, economic, and social context can determine whether a specific system will cause benefit or harm. However, evidence has shown that digital ID systems with certain characteristics are more likely to raise human rights concerns. This includes systems designed to be foundational, interoperable, or multi-purpose, systems linked to determinations of nationality and legal identity, and systems that incorporate the use of digitized biometric data. The recommendations of the HR4ID coalition are especially relevant for systems with one or more of these characteristics, but apply to all forms of digital ID.

This position reflects our current understanding, drawing on the work, knowledge, and perspectives of coalition members and the diverse communities in which we work. All digital ID systems, and especially those introduced by public institutions, should be responsive to the needs of affected individuals and communities. Therefore, we encourage public institutions to turn away from imposing mandatory requirements that all too often lead to expansive data collection and the misuse of identifying technologies, and instead to design and build digital infrastructures that embrace autonomy, equality, and dignity.

Introduction and Key Concepts

In national contexts around the world, both public and private institutions increasingly require individuals to enroll in digital ID systems, as well as to use these systems in order to access services, processes, or online and offline spaces.[i] Often digital ID is introduced for specific purposes, such as making service delivery more efficient and reducing public expenditure, increasing the security of online transactions and reducing fraud, facilitating democratic processes such as elections and access to justice, or improving national security. However, under certain circumstances, these digital ID systems can heighten the risk of exclusion and discrimination, violate privacy rights, and create sociotechnical systems that facilitate the overcollection and misuse of data. In making such systems *mandatory*, these harmful impacts can be accelerated, scaled, and intensified.

Moreover, digital ID systems are prone to function creep, which means that their powerful sorting and identifying capabilities—as well as the large amounts of underlying personal data that they collect—may be used and misused for different purposes over time.[ii] This raises significant concerns about the potential for abusive or coercive use of identifying technologies and data, both by public institutions and also by the private sector. Therefore, such systems may not only immediately impact the lives and rights of marginalized groups, but also heighten the risk of harm to entire populations over time.

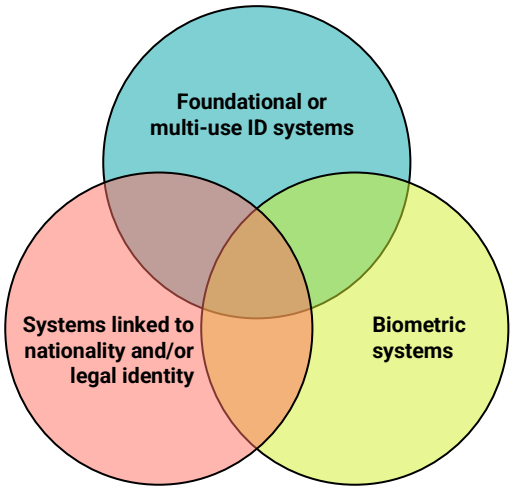
Members of the Human Rights for Digital Identity (HR4ID) Coalition work on an array of topics related to digital ID, human rights, and social justice in diverse local contexts around the world, and our members include grassroots, community-based organizations, national and international civil society organizations, and academic researchers and independent experts.[iii] Drawing on our work with affected communities, this position statement highlights our urgent concern about the harmful impacts of mandatory digital ID requirements. It is intended to be a living document that will evolve based on new evidence, policies, and solutions, but will always maintain the central aim of encouraging the development of digital ecosystems that promote autonomy, equality, dignity and the full enjoyment of human rights for all.

Digital identification systems are only one part of a person's digital identity

Our understanding of *digital identity* covers initiatives, systems, policies and practices that sit at the intersection of individuals (and groups of individuals), on one hand, and public and private entities that hold institutionalized political and economic power, on the other. We see digital identity as a medium of recognition, autonomy and agency for members of the public that is still taking shape and holds massive implications for the future of citizenship, social and economic justice, democracy and the rule of law.

This position statement is specifically concerned with *digital identification systems* that are created, supported, or used by public institutions for the purposes of identifying, enrolling, authenticating, and authorizing access to online and offline services, spaces, and processes.[iv] While digital ID systems can help to support and shape the expression of digital identity, they are merely one facet of an individual's online self. Examples of digital ID systems may include official digital ID cards, civil documentation that incorporate digital components, IDs linked to private companies and mixed public and private identification systems. This definition encompasses initiatives described as verified credentials, digital public goods, digital public infrastructure, digital transformation, and modernization of service delivery through digital means.

Public and private actors are currently experimenting with new approaches to technology, administration, and governance, which has led to the introduction of different forms of digital ID. Most notably, growing interest in digital public infrastructure initiatives has led to a flurry of activity to define new national approaches to digital ID,[v] as well as to create systems for the governance of new systems. However, given the current limitations of digital identification systems— most notably the potential for such systems to facilitate direct and indirect discrimination and exclusion—requiring the mandatory use of any *single form* of digital ID system has the potential to negatively impact individuals and communities lacking access to these documents. Therefore, careful, context-based consideration must be given to the legality, necessity, and proportionality of making such systems mandatory.



Some types of digital ID systems are particularly concerning

We argue that there is compelling evidence that certain types of digital ID systems, due to their design and implementation, significantly increase the risk of harmful outcomes. Making these types of systems mandatory for access to public services and fundamental rights can negatively impact human life, particularly for vulnerable and marginalized groups. We are particularly concerned about three–sometimes overlapping–types of systems:

1. **Foundational or multi-purpose digital ID systems,** which are not limited to a particular purpose or functional area. These systems are often population scale infrastructures, which are designed to provide identification services for multiple purposes. Rather than being fixed from the outset, the purpose, users, and relying parties who use these systems are intended to evolve over time. Moreover, these systems are often designed to be interoperable,[vi] with the technological capability to easily share data between both public and private institutions. Therefore, while foundational digital ID systems are primarily developed, deployed and governed by public institutions, private and non-governmental organizations may be involved at various stages of their development, operation, and use; for instance, Big Tech companies can both provide ID solutions, such as digital wallets, and also make use of publicly provided infrastructure. This makes such systems particularly susceptible to function creep,[vii] with novel—and potentially harmful—use cases emerging over time. Examples of foundational digital ID systems include Aadhaar unique identification system in India; the Ndaga Muntu national digital ID system in Uganda; the Cédula de Ciudadanía Digital in Colombia; and Huduma Namba / Maisha Namba in Kenya.

2. **Digital ID systems that are linked to determinations of nationality and conferral of legal identity**. These systems may limit enrollment to those who are able to provide proof of nationality or differentiate between those who can and cannot provide proof of nationality. They may also be linked to systems of birth registration that help to constitute legal identity or collect data that can be used to make inferences about citizenship, legal recognition, and other entitlements associated with legal identity. For instance, the National Integrated Identity Management System (NIIMS) was designed to integrate Kenyans digital identity, but this required proof of identification cards and disproportionately affected the Nubian, Somalis and other minority groups, who had been historically excluded from accessing forms of official identification.

3. **Digital ID systems that rely on digitised biometrics in order to enroll, identify, authenticate, and authorize users.** These systems often require individuals to provide biometric data in order to enroll in and use the system. In some instances they can instead make use of biometric data originally gathered for a different purpose, which is then re-purposed for identification, authentication, or authorization purposes. Given the immutable nature of biometric data—and combined with the interoperability of data—these systems are capable of consolidating multiple sources of data, transforming into highly invasive, multi-purpose data infrastructures. For instance, the Aadhaar system in India uses digitized fingerprints, iris scans, and facial recognition to de-duplicate records and to perform processes of identification, authentication and authorization.

Significant human rights violations can be associated with digital ID systems

Digital ID systems that have one or more of these characteristics are of concern because of their ability to identify individuals based on personal characteristics, to facilitate decisions about who can and who cannot have access to certain rights, services, processes, and online and offline spaces, and the ways in which they amass large amounts of personal data in interoperable systems that can be accessed and used by multiple actors. These functions—identification, access, and multi-purpose interoperable data systems—have had a demonstrable, harmful impact on marginalized and vulnerable populations in many countries where digital IDs are in use.

The serious harms caused or facilitated by these systems can include, for instance, discriminatory vetting practices that deny access to forms of legal identity,[viii] or being excluded from public services like health care and social security for lacking a digital ID.[ix] Equally concerning is what these systems can mean for those who *are* included. Since such systems can lead to the overcollection of data, this can in turn lead to violations of privacy and data protection. The combination of the sorting capabilities of digital ID systems with the large amounts of data that digital ID systems help to collect, organize, and use provides a powerful tool that can be used to surveil, coerce, discriminate, and persecute. This can lead to practices such as ID blocking,[x] surveillance of minority groups[xi] and people living in poverty, and the persecution of human rights activists or political dissidents through forced disappearances and abductions. Meanwhile, the interoperability of data and potential for function creep mean that new threats can continue to arise the longer a system is in place.

Different types of mandatory requirements contribute to harm

In this document, we reference two related forms of mandatory requirements: mandatory *enrollment*, where individuals are required to register and successfully enroll in a specific digital ID system, and mandatory *use*, where having a specific digital ID becomes a necessary precondition for access to services (public and private), online and offline spaces (i.e. online platforms and physical free movement), or processes (i.e. legal procedures and voting).

Both types of mandatory requirements can be codified in law or state/public policy (*mandatory in law)*. However, these requirements can also emerge indirectly as the result of practices that make it necessary to have a digital ID in order to fully exercise human rights (*mandatory in fact)*, even in systems that appear to be voluntary. Mandatory in fact requirements can include: making a specific digital ID the default option while making it more difficult or inconvenient to use alternative forms of ID; withdrawing support for alternative forms of ID, such as limiting access to previously available paper-based or functional forms of ID; or allowing third parties, including private actors, to impose digital ID

as necessary preconditions for accessing their services. Different aspects of a digital ID system can be mandatory; for instance, some data, such as nationality or gender, may be required fields in the digital system in order to successfully register, even if such information is not explicitly mandated in law.

The potentially harmful effects of mandatory digital ID requirements often arise because of complex social, technological, economic, and political factors. It is critical both to understand the ways in which mandatory digital ID requirements can alternatively reflect, improve, or worsen existing dynamics.[xii] However, across these different contexts it remains the State's duty, through their public institutions, to ensure that digital ID systems fully comply with human rights law, principles and standards, including those related to legality, proportionality and necessity for a clearly articulated legitimate goal in their design and implementation.[xiii] Additionally, public institutions have a responsibility to be attentive not only to the prospective benefits of digital ID systems, but also to their potential negative impacts; this means actioning appropriate policy and technological changes to address issues as they arise, and implementing adequate remedies for those who have been harmed.

Our common position on mandatory digital ID requirements

Our recommendations are based on the severity of human rights concerns posed by mandatory digital ID systems, the persistent obligations of the State to realize human rights equally for all, and the legitimate purpose of building digital ecosystems that are rooted in autonomy, equality, and human dignity.

1. Mandatory digital ID requirements negatively impact human rights and human life, particularly for those who are marginalized or vulnerable.

Mandatory digital ID *enrollment* requirements can have severe consequences on individuals' ability to exercise their human rights. Those who are unable or unwilling to comply with enrollment requirements may be subject to fees or penalties, as well as stigmatization and discriminatory treatment. Mandatory enrollment requirements can also lead to excessive data collection, creating the potential for function creep,[xiv] as well as different forms of misuse and abuse.

Mandatory use requirements can worsen these impacts, because those who are not enrolled in the digital ID system are then excluded from accessing further services, online and offline spaces, or processes. Mandatory use requirements can also enable forms of direct and indirect discrimination even for those who have been able to successfully register. For instance, the data collected can facilitate differential treatment of individuals with certain characteristics. These forms of exclusion and discrimination severely infringe on human life, affecting economic and social rights, equality and non-discrimination, legal recognition, self determination, free movement, free expression, privacy, dignity, autonomy, and nationality.

Both *mandatory enrollment* and *mandatory use* requirements have been shown to particularly affect vulnerable and marginalized groups, including: ethnic, religious, racial or national minorities; stateless persons; migrants; Human Rights Defenders; Persons with Disabilities; women and girls; displaced persons, refugees, and asylum seekers; and people living in poverty. Other groups have been subject to surveillance through the use of digital systems,

such as sex workers, persons living with HIV, and drug users. Members of these groups may disproportionately bear the harm of these systems, and often face more stringent barriers to access, harsher consequences for non-compliance, and targeted mistreatment throughout the digital ID enrollment and use process.

2. Public institutions[xv] should not require mandatory enrollment in a digital ID system.

There are many reasons why individuals may be unable to comply with mandatory digital ID enrollment requirements, and therefore be excluded from the system. Since digital ID enrollment processes often draw on existing legal, administrative, and political processes of identification, as well as access to technologies and skills required for registration (including smartphones, connectivity and digital literacy), they can replicate inequalities and reinforce discriminatory practices. This includes direct discrimination through practices such as limiting registration to certain social, cultural, or ethnic groups, or making enrollment contingent on providing artefacts such as birth certificates, which are not equally available and accessible. This also includes indirect discrimination through practices such as establishing registration points in inaccessible physical locations, the required use of majority languages, and the imposition of high fees and other financial barriers that can frustrate enrollment for those living in poverty. Moreover, enrollment processes are often dependent on physical infrastructure, such as roads or transport, electricity, and mobile or internet coverage, which are not equally accessible.

When digital ID enrollment is mandatory, these practices and contextual factors lead to a heavy burden on individuals and communities to prove their identity to public and private institutions, while simultaneously limiting autonomy and agency to form one's legal identity and digital footprint in the manner that one chooses.

There may also be individuals who have legitimate reasons to resist registration, for fear of surveillance, repression or persecution. Furthermore, any form of population scale collection of biometric data (whether fingerprints, iris scans or facial images) entails severe risks for the privacy of individuals, especially for systems that are designed to be multi-purpose. By imposing a mandatory digital ID enrollment requirement, the State effectively eliminates choice and consent in the initial processes of identification and creates the potential for further violations.

3. Public institutions[xvi] should not require mandatory use of elements of the digital ID system to access public services or privately provided public services.

Beyond the enrollment stage, mandatory digital ID use requirements often lead to the exclusion of those who have been unable or unwilling to enroll in the digital ID system, as well as those who have errors in their digital ID or face barriers in fully using the system. By making it mandatory to use a digital ID, both public and private institutions can erect discriminatory barriers and exclude individuals from public and privately provided public services.[xvii] This includes healthcare, voting, education, social security, and legal recognition, but can also include SIM cards, access to the labor market, and online platforms. Mandatory use requirements can also be used to limit free movement, both within national territories

and across borders, especially in cases where mandatory use is combined with transnational data sharing.

Mandatory use requirements also enable forms of direct discrimination against certain groups, even those who have successfully enrolled in the digital ID system, through the collection, sharing, and use of personal data. As digital ID systems become more embedded, these requirements lead to the risk of function creep, as well as misuse and abuse by both public and private actors. The consequences of being enrolled in the system, as well as being required to maintain and use a specific form of digital ID, means that accumulated data can be exploited to target individuals for mistreatment.

Elements of the digital ID system can also be weaponized by freezing ID cards, numbers, or profiles; limiting access to certain processes, spaces or services based on personal characteristics such as gender identity, ethnicity, or location; or using personal identity information to introduce forms of algorithmic profiling. In some of the most severe cases, mandatory data collection and use can be used to single out political dissidents, human rights defenders, journalists, and other marginalised groups, leaving them vulnerable to disproportionate surveillance, censorship, intimidation, or even extrajudicial killings and other forms of state violence. All too often, there are little to no remedies available for those who suffer the effects of digital ID systems.

4. In contexts where digital ID systems already exist or are in development, the State has an obligation to guarantee that equal, adequate, and accessible alternatives are available–including non-digital alternatives–for those who are not enrolled or who do not use the digital ID.

Whenever a digital ID system is in use the State has an obligation to guarantee that adequate safeguards are in place to ensure protection and realization of human rights; this applies equally to systems that are mandatory and systems that are voluntary. However, as described in the sections above, mandatory digital ID enrollment and use can lead to significant violations of human rights and have a profound impact on human life. These harms can outweigh the intended benefits of imposing a mandatory requirement, such as encouraging enrollment and collecting vital statistics, calling into question the necessity, proportionality, and legality of mandatory digital ID requirements.

The most effective way to mitigate the numerous human rights issues is for the State to ensure that there are equal, accessible, and adequate alternatives available in order to access services and to enjoy fundamental rights. Creating and sustaining alternative means of identification ensures that there will be multiple legitimate pathways for individuals to access services, spaces, and processes in a way that meets their needs. This reduces the risk of exclusion and discrimination and preserves individual autonomy and dignity. Allowing the use of alternatives also mitigates the potential risk of privacy violations and overcollection, misuse, and abuse of data, while safeguarding against long-term systemic risks of function creep that comes with reliance on a single system. As an example, the EU has established a legal obligation to ensure alternatives to digital ID are available for all public services, the private sector and the labor market, as well as a prohibition against discriminations of non-users in these sectors.[xviii]

In determining which alternatives are equal, adequate, and accessible, public institutions should take into account contextual factors such as existing discriminatory laws and practices, access to digital infrastructure and tools, availability and accessibility of

alternative sources of identification, and the level of assurance necessary for those who seek to verify a person's digital identity. Many countries face common challenges such as legal and administrative barriers to accessing systems of identification, unequal levels of digital literacy and access to digital infrastructure, and the lack of universal, equitable coverage for digital ID systems. Therefore, in the current context, public institutions must ensure that these alternatives include non-digital options for those who are not enrolled in or who do not use the digital ID system. For instance, withdrawing or reducing support for alternative forms of identification, including paper-based digital ID systems, can lead to digital ID systems becoming mandatory in fact. This, in turn, can lead to many of the issues described above for those who do not use the digital ID system.

While non-digital alternatives are necessary to safeguard equal access in the short-term, there remains a risk of creating stratified systems, where one dominant system benefits the majority and alternative systems provide more limited, constrained access to those who remain marginalized. Given the importance of context in determining the most appropriate solutions, we encourage states to consult directly with civil society organizations and provide opportunities for the participation of affected communities to seek long-term solutions that foster autonomy, equality, and dignity, while finding ways to use digital technology to meet the needs of administration, governance, and sustainable development.

Conclusion

Mandatory requirements to enroll in or use a specific system have been shown to disproportionately harm marginalized and vulnerable individuals and communities. Not only can this have a profound impact on the ability to enjoy fundamental human rights, it may also alter the relationships of public institutions with diverse individuals and communities and lead to long-term, transformative harm. This frustrates the very goals of sustainable development and human rights that are used to justify public investment in national digital ID systems. We encourage public institutions to turn away from imposing mandatory requirements that all too often lead to expansive data collection and the misuse of identifying technologies, and instead to design and build digital infrastructures that embrace autonomy, equality, and dignity.

When it comes to digital identity, we believe that the starting point should not be the need to create new or updated digital identification systems, but instead the best way to meet both the positive and negative obligations to ensure full enjoyment of human rights for all. We encourage public institutions to recognize that investments in non-digital infrastructure and non-digital services—as well as legal, regulatory, and administrative frameworks that encompass key concerns such as data protection and remedies for digital harm—may play an equally or more important role in realizing human rights for all. And most importantly, public institutions must take affirmative steps to ensure that these digital systems remain truly voluntary–with equal, adequate, and accessible alternatives for those who do not or cannot access these systems.

End Notes

[i] The Human Rights for Digital Identity Coalition is currently mapping an overview of national legislation on digital ID. This map will be published on the coalition's forthcoming website.

[ii] While many digital ID systems are still in the process of being introduced or updated, experience in countries where digital ID systems have been in place for decades demonstrates how the use cases of these systems can evolve over time, raising concerns such as changing discriminatory patterns, private sector capture, and political weaponization of the digital ID against minority groups. *See, e.g.*, Sandhu & Balakumaran, Function Creep and FinTech in India: The Aadhar ID System (Part 1: Trading Faces), REal Media, 16 May 2017, https://realmedia.press/function-creep-fintech-india-aadhar-id-system-part-1-trading-faces/.

[iii] For more information about the coalition, please email admin@hr4id.org.

[iv] For discussion of the types of identification technologies, see Immigrant Defense Project, Understanding the Risks of Digital IDs, 2023, https://surveillanceresistancelab.org/wp-content/uploads/2023/01/Digital-IDs-FAQ.pdf; Center for Human Rights & Global Justice and Institute for Law, Innovation & Technology, Shaping Digital Identity Standards, 2023, at https://law.temple.edu/ilit/shaping-digital-identity-standards/; Centre for Internet and Society, Core Concepts and Processes, 2019, at https://digitalid.design/core-concepts-processes.html.

[v] For ongoing efforts to map these efforts, see UCL Institute for Innovation and Public Purpose, Global DPI Map, at https://dpimap.org/global-state-of-dpi.

[vi] Interoperability is seen as a critical component of digital public infrastructure, and can be understood as the ability of different organisations or units to share information and knowledge. Interoperability can have a legal, organisational, semantic, and technical component. *See* EU Interoperability Framework, 2017, at https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf.

[vii] We use the term function creep to describe the process by which digital ID systems, through either their identifying technologies or their underlying data, are increasingly used to determine eligibility or access to different services, processes, or online and offline spaces, often without determining whether such use is legal, necessary, or proportionate. For examples of how digital ID system function creep can lead to harm, see Mizue Aizeki & Rashida Richardson, eds., Smart-City Digital ID Projects: Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions", New York, NY: Immigrant Defense Project, December 2021, at https://law.northeastern.edu/wp-content/uploads/2021/12/clic-smart-city-report.pdf,

[viii] Namati, Kenyan Government Reforms ID Vetting; Abolishes Vetting Committees, April 2, 2025, at https://namati.org/news-stories/kenyan-government-reforms-id-vetting-abolishes-vetting-committees/

[ix] Jose Arrazia, *Will Digital ID Help Stateless People? The Threat of Digital Administrative Violence*, European Network on Statelessness (2023), https://www.statelessness.eu/updates/blog/will-digital-id-help-stateless-people-threat-digital-administrative-violence (last visited May 12, 2025); Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness, Chased Away and Left to Die: How A National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons (2021), https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf.

[x] Assam citizenship crisis: Aadhaar unlocked, lives shackled, CJP (2024), https://cjp.org.in/assam-citizenship-crisis-aadhaar-unlocked-lives-shackled.

[xi] Digital Surveillance and the Threat to Civil Liberties in India, Hamburg: German Institute for Global and Area Studies (GIGA) (2021), https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india.

[xii] For instance, digital ID systems can pose unique risks in specific contexts, such as conflict-affected regions or fragile states, as well as for specific populations such as people living in poverty, stateless persons, and refugees and asylum seekers.

[xiii] Privacy International, Legality, Necessity and Proportionality, at https://privacyinternational.org/our-demands/legality-necessity-and-proportionality; Centre for Internet and Society, Governing ID: a Framework for Evaluation, at https://digitalid.design/evaluation-framework-02.html; Amicus brief of Prof. Philip Alston, *ISER & Others v. Attorney General & Another, High Court of Uganda at Kampala,* 19 September 2022, at https://drive.google.com/file/d/1dsQKveamxwzINZmAHp8bs4zajYdXVHIN/view.

[xiv] *See note 6.*

[xv] We use the term "public institutions" to encompass the variety of departments, agencies and other bodies that are responsible for governing, administering and using digital ID systems in different countries. This term can include both institutions of the state, but also quasi- and non-state bodies that are responsible for administering public services.

[xvi] See note 4.

[xvii] While our focus is on public institutions, many national approaches to digital ID and public service delivery include the involvement of private sector actors, whether through public-private partnerships, the support of private consultants or technology vendors, or through private use of public infrastructure. The involvement of private actors poses specific risks. *See* Mutung'u G. The United Nations Guiding Principles on Business and Human Rights, Women and Digital ID in Kenya: A Decolonial Perspective. *Business and Human Rights Journal*. 2022;7(1):117-133, at doi:10.1017/bhj.2021.60.

[xviii] Epicenter.works, Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures, 29 February 2024, at https://epicenter.works/en/content/analysis-of-privacy-by-design-eu-legislation-on-digital-public-infrastructures