moz://a

WHITE PAPER

Bringing Openness To Identity

Technical And Policy Choices For Open National ID Systems

Amba Kak, Jochai Ben-Avie,
Alice Munyua, and Udbhav Tiwari

Contents

EXECUTIVE SUMMARY

LIVING OUR ONLINE AND OFFLINE LIVES increasingly requires either identifying yourself or being identified. Social login services which let you login with Facebook, ad IDs that are used to target ads to you, or an Apple ID that connects your text messages, music preferences, app purchases, and payments to a single identifier are all examples. While we can and should be concerned by how private companies are using identity systems to amass vast databases about us, many governments are already several steps ahead. In many countries, people are being required to use a singular government issued digital -- and often biometric -- ID in order to get food rations, get treated in a hospital, or get a cellphone connection all logged in a centralized government database. Too often, these identity systems are being deployed in developing countries which lack data protection laws or robust connectivity infrastructure.

Part of the push to adopt digital ID comes from international development community who argue this is necessary in order to expand access to *legal* ID. The UN Sustainable Development Goals (SDGs) call for *"providing legal identity for all, including birth registration"* by 2030. Possessing legal identity is increasingly a precondition to accessing basic services and entitlements from both state and private services. Without these commonly recognized forms of official identification, individuals are at risk of exclusion and denial of services. However, the conflation of digital identity as the same as (or an extension of) "legal identity", especially by the international development community, has led to an often uncritical embrace of digital ID projects.

The digital features and networked infrastructure of these ID projects have very different implications from their analog counterparts. For example, they often: contain deeply sensitive information (biometrics or even DNA), allow for linking ID numbers across many databases, enable enhanced surveillance through the centralized collection of data, and rely on electricity and connectivity for real time authentication which are often unreliable, exacerbating exclusion.

The digital features and networked infrastructure of these ID projects have very different implications from their analog counterparts.

Debates around digital identity have forced questions on: the appropriate use of biometrics; the amplification of surveillance through the linking of databases; experimentation with tech in low-rights environments (e.g., in countries without data protection laws or enforcement); and the lack of consultation in the design of technology projects. Many of these issues overlap with broader concerns around the internet and emerging technologies like AI.

In designing, implementing, and operating digital ID systems, governments must make a series of technical and policy choices. It is these choices that largely determine if an ID system will be empowering or exploitative and exclusionary. While several organizations have published principles around digital identity, too often they don't act as a meaningful constraint on the relentless push to expand digital identity around the world. In this paper, we propose that openness provides a useful framework to guide and critique these choices, and to ensure that identity systems put people first. Specifically, we examine and make recommendations around **five elements of openness: multiplicity of choices, decentralization, accountability, inclusion, and participation.**

We conclude the paper with the following recommendations:

- Governments must conduct wide ranging consultation on the technical and policy choices involved in the ID systems from the design stage of the project. The collection and use of biometrics in any identity system comes with significant privacy risks and should be carefully considered in an open, consultative, and evidence-based process. It is critical to consider factors such as infrastructure, connectivity, occupation, and digital literacy, as well as institutional, social, and political histories of identification in a country.

- A multiplicity of choices in the use and possession of IDs should be available to people to support the sharing of key identity attributes, rather than the imposition of a single, rigid and mandatory ID system for all purposes.

- Digital IDs should be designed from their inception to prevent their use as a tool to enable and amplify government and private surveillance. Countries should critically examine whether logging of authentication requests is needed at all, and should certainly put into place laws to limit the retention, accessing, and sharing of authentication records. This process of authentication can create a digital record of where and when the individual uses their ID. The presence of such authentication records poses also significant privacy and security risks along with increasing the potential for surveillance.

- The use of national ID numbers retained in the databases of private companies can be used to profile and discriminate between citizens. This usage must be publicly debated and regulated. The ability to cross-link databases through the use of the ID credentials can significantly enhance the tracking capabilities of private companies and should be prohibited or at a minimum governed by law. The creation of private ecosystems on top of government IDs (particularly those with open APIs) must be closely scrutinized, particularly for applications that use personal data in predatory ways.

- Data protection laws should be in force, with a strong, independent regulator, before the roll out of any national biometric ID project.

- ID systems must be technically auditable by independent external bodies to ensure trust, security, and inclusion. Audits should be conducted to ensure that the ID system complies technically with the legal frameworks governing the system and personal data. We also recommend all national ID systems should be open sourced as this will improve transparency of such systems and ensure their outcomes are verifiable against audits.

- Verifiable inclusion should be a core pillar in the design of digital ID systems. No one should be excluded based on de-

mographic or physical characteristics. Identity systems must account for digital literacy levels of populations and must be resilient in the face of low connectivity environments. Individuals must not be denied essential services because they don't have a particular ID or the system did not function.

- Individuals must have the ability to opt out of certain kinds of data sharing when using their IDs, especially around sensitive information that might cause harm if disclosed.

INTRODUCTION

DIGITAL IDENTITY has many meanings today. The proliferation of digital networks has led to a range of new identifiers in the form of email addresses, phone numbers, handles on social messaging, and social media services, controlled by some of the largest internet companies (Google, Facebook, Twitter, Linkedin). Today, an increasing number of these companies also offer to become "identity providers" for users across their interactions on the web. Every time someone decides to "login with Facebook" (or Google, or LinkedIn) on a website or application, for example, these companies are inserted into those transactions, and the related data trails. These data trails of user behavior online form profiles, which are themselves a kind of digital identity. These digital identities are a valuable resource for a range of actors from social media companies to advertising networks who use them as a way to target and personalize content and marketing to users.

Meanwhile, governments, the more traditional "ID providers" are transforming the nature of their ID systems by either upgrading their analog ID systems to digital ones, or creating new, entirely digital networked ID systems. A prominent model is one which requires citizens to enroll multi-model biometrics (fingerprints, iris scans, and photographs) in order to obtain a unique identity number. To access services through these systems individuals are then asked to share both the number and their biometrics (like fingerprints), which are often sent electronically to a centralized database to check if it matches the one on file. This process of authentication can create a digital record of where and when the individual uses their ID. In fact, even as we continue to debate the value of anonymity online and how to safeguard privacy appropriately, governments globally are surging ahead to institute digital systems to identify and track residents across their online *and* offline lives.

Mozilla is deeply invested in how technology can be harnessed for public benefit and to enrich the lives of human beings. Debates around digital identity bring this issue to the fore. It has forced questions on the appropriate use of biometrics; the amplification of surveillance through the linking of databases; experimentation with tech in low-rights environments (for example, in countries without data protection laws or enforcement); and the lack of consultation in the design of technology projects. Many of these issues overlap with broader concerns around the internet and emerging technologies like AI.

This position paper will look specifically at the context of governmental digital ID projects, drawing heavily from the experiences in India and Kenya, and referencing the experiences of Estonia and British Columbia, among others. In the last few years, we have seen multiple governments across the world announce and roll-out digital, national level, and general-purpose ID projects. These have come in various forms, from chip-based smart cards with biometric data to unique number based systems to those that use mobile-based identification and authentication. Government-issued digital IDs are often mandatory for residents to get access to welfare and other services, making the real impact palpable for every citizen. For the most marginalized communities, ID systems are often one of their first interactions with digital technologies.

1.
BACKGROUND ISSUES AND CONTEXT-SETTING

1.1 LEGAL IDENTITY V. DIGITAL IDENTITY

THE UN SUSTAINABLE DEVELOPMENT GOALS (SDGs) call for *"providing legal identity for all, including birth registration"* by 2030. Possessing legal identity is increasingly a precondition to accessing basic services and entitlements from both state and private services. Without these commonly recognized forms of official identification, individuals are at risk of exclusion and denial of services.

However, the conflation of digital identity as the same as (or an extension of) "legal identity", especially by the international development community, has led to an often uncritical embrace of digital ID projects. The digital features and networked infrastructure of these ID projects have very different implications from their analog counterparts. For example, they often:

- ▷ Contain sensitive personal information like biometrics or even DNA profiles;
- ▷ Allow for electronically linking ID numbers across connected databases;

- ▷ Enhance search and sorting capacities based on demographic criteria; and
- ▷ Rely on electricity and connectivity for real time authentication, which are often unreliable;

These digital attributes are generally advocated as a means to more efficient enrollment and authentication, and less prone to fraud than their analog counterparts. As the experience from various countries has borne out, however, these so-called efficiencies will vary entirely with the context in which they are deployed. Moreover, digital and biometric systems raise new kinds of concerns and dangers which we explore in the sections below. Every claim of efficiency and security must be subject to close scrutiny and we must be prepared to question *if* not just how digital technologies are appropriate for ID systems.

1.2 SURVEILLANCE AND DIGITAL ID

IDENTITY SYSTEMS raise questions about the appropriate limits of government surveillance. From logging onto a WiFi hotspot to buying a train ticket to making a doctors appointment, when a wide range of services require the same unique number and authentication via its centralized system, the state gains access to an intricate record of an individual's movements, activities, and affiliations. Even where the ID number itself is not linked to sensitive information, its ability to uniquely identify individuals across databases can generate sensitive inferences. In India, state governments created a public online dashboard of residents that was searchable by religion and caste[1], by simply combining various discrete databases that were seeded with the Aadhaar number (India's mandatory biometric-linked identity number).

The ability of identity systems to facilitate and aid government surveillance is often implicit, but sometimes even a stated goal of these projects. In India, the Supreme Court struck down the legal provision that allowed disclosure of authentication records for government surveillance on the grounds that there was weak executive

review and could lead to “misuse of power”. In Mexico[2] and Pakistan, anti-terrorism and law and order are stated objectives of the national identity projects. Pakistan’s ID database, NADRA, has been linked[3] to the database of criminals and is routinely used in criminal investigations.

Beyond government, there is also potential for private companies to take advantage of the surveillance capability of ID systems. Take for example, India’s digital ID system based on an open API system that allows for public and private uses. Whether it was telecom companies[4], banks, or background verification[5], or as we uncovered, tracking lost Amazon packages[6], an increasing number of services began to require Aadhaar numbers. While these companies don’t necessarily get visibility into the individual’s complete authentication record, they still retain records of the ID number which can then be combined with similar databases from other businesses and services. Eventually, this allows for easier cross-linking of databases and enables profiling of individuals at scale. In September 2018, the Supreme Court of India placed several limits[7] on the ubiquitous use of Aadhaar by private companies, in part due to these foreseeable privacy risks.

Beyond government, there is also potential for private companies to take advantage of the surveillance capability of ID systems. Take for example, India’s digital ID system based on an open API system that allows for public and private uses.

1.3 FOCUS ON DEVELOPING COUNTRIES

THE WORLD BANK alone has supported no fewer than 63 ID projects[8] in developing countries in the past 15 years, and these efforts are only growing. While countries across the development spectrum are implementing digital IDs, there appears to be deliberate efforts in the international development community to encourage[9] developing countries to upgrade or "leapfrog" to these technologies.

David Lyon (2009)[10] notes that almost all developed countries have seen national biometric ID projects involving more than photographs[11] opposed and eventually defeated, including on grounds of privacy, for example, in the USA[12], the UK[13], Canada[14], France[15], and Australia[16]. In developing countries, although local and international civil society groups have been actively pushing back to raise concerns, they have often been too late to influence structural changes in the design of these projects. The legal framework for India's ID project came after large parts of the population were already enrolled, while in Kenya, a law was passed authorizing the collection of biometrics (including DNA) as part of a new digital ID system with no prior public notice or debate. Public consultation is critical to engage affected stakeholders as well as civil society groups. While India and Tunisia[17] saw wide-ranging protests and activism around the ID project despite weak consultation processes, and the Jamaican Supreme Court ruled their ID project wholly unconstitutional, many countries are unlikely to benefit from such a robust civil society or judicial response.

Despite weak legal norms (and limited track records of enforcement) of data protection, it is concerning to see so many digital ID efforts in developing countries across Asia, Latin America, and Africa. Several countries have implemented digital ID systems without any laws in place to regulate government use of personal data, including India, Kenya, Nigeria, and Malaysia. Governments and donor organizations must account for these specific legal and institutional realities when evaluating the potential impact of national ID systems.

1.4 EXISTING PRINCIPLE-BASED APPROACHES

A RECENT STUDY (New America, 2018[18]) compares the various principle-based frameworks for ID ranging from international organizations (World Bank[19], World Economic Forum[20]) to civil society actors (Access Now[21]) and individual experts (Kim Cameron[22], Christopher Allen[23]). To varying degrees, there is a welcome emphasis on privacy and security as a core value in these frameworks, as well as a focus on the universality and accessibility of IDs across socio-economic disparities.

We hope to supplement these efforts primarily in two directions:

- *First,* while openness is recognized as a value in some of these frameworks,[24] it is almost exclusively in terms of interoperability -- specifically, the use of either open APIs or open standards for IDs to prevent vendor lock-in[25]. However, openness in the context of ID should be broader than just this limited definition. It should encompass both a broader range of technical guidance, but also, critically, a preference for social, legal, and policy choices that best empower the individual user. In the following sections, we make the case for where values of openness can more holistically guide the debate on digital ID.

- *Second,* while these principles all generally acknowledge privacy should be central to the conversation around digital ID, we identify some critical guardrails to achieve this goal, especially in the context of developing countries.

2.
OPEN NATIONAL IDENTITY SYSTEMS

ALL DIGITAL ID SYSTEMS are the result of a series of technical and policy design choices. Considering several key aspects of openness provides a useful frame for making design choices that put (and keep) people at the center of these systems. Specifically, we have identified five facets of openness that relate to the debate on national IDs: multiplicity of choices, decentralization, accountability, inclusion, and participation.

2.1 OPEN AS IN A MULTIPLICITY OF CHOICES

AN INDIVIDUAL SHOULD HAVE a multiplicity of choices of how to present key attributes that compose their identity rather than the imposition of a single and rigid system. However, choices over what ID to use are often rendered illusory either in fact or by law. This is especially true for centralized national ID systems, since governments often have the power to require national IDs for a range of essential public (and sometimes private) services.

Individuals should generally have the ability to reveal only specific, relevant attributes associated with their identity depending on the legitimate requirements of the context. The counter-argument is that a “foundational” ID system that has broad (rather than specific) functionality brings with it significant benefits in terms of convenience, accessibility, and ease of use. While these are important values to consider, this should not be an excuse to coerce those who are reluctant to use the same ID across contexts. In several countries, the push for a single ID system has meant that pre-existing IDs have been rendered obsolete, often overnight, leading to restricted choices for users.

Another byproduct of imposing a single centralized system across contexts is a single authentication record (a record of all usages of the ID) that reveals a detailed profile of every individual and their actions, compromising privacy and creating a serious security risk. Systems should be designed to optimize individual agency and flexibility across contexts.

The consequences of insisting on a single ID issued by a centralized authority, rather than relying on a demand-driven approach, can be dire, as the experiences in both Peru and India demonstrate. In Peru[26], in 2012, enrollment in a government health welfare program dropped dramatically when having the state ID was made mandatory for children, eventually leading to higher child malnutrition in some of the targeted areas. In the case of India's Aadhaar system, although stated to be strictly voluntary, we saw the ID became a precondition to access many essential public and private services, leading to a de facto single standard where prior IDs were no longer in use. In several tragic cases[27] in India, people died of starvation because they could not get their food rations because they either didn't have the Aadhaar or the system lacked the functionality,

The consequences of insisting on a single ID issued by a centralized authority, rather than relying on a demand-driven approach, can be dire, as the experiences in both Peru and India demonstrate.

electricity, or connectivity to work. Notably, in both Peru and India, the law did allow for alternatives to prevent such denial of services (e.g., using another form of government-issued ID), but these instructions didn't filter down to the administrators on the ground.

More broadly, we are concerned by projects that seeks to arrive at the "single" right model of ID. The World Bank ID principles, for example, put forth many progressive values of privacy, security, and interoperability. However, they are formulated to suggest *"a"* robust identity and *"a"* single platform rather than a system that is capable of deriving attributes and identity from a multiplicity of authoritative sources as is true in the real world as well. We should keep choice and the absence of coercion central as we debate better, and worse, forms of digital identity.

2.2 OPEN AS IN DECENTRALIZED

NATIONAL ID PROJECTS have generally been centralized by design, where authentication involves a citizen presenting a number that is then looked up in a government's centralized database with the user considered authenticated if the factor of authentication that is presented matches that on file. If they enrolled fingerprint biometrics, for example, it would be whether the fingerprint matches. Often the goal of these systems is to create IDs that can be used for virtually all identification purposes. In the context of Aadhaar, Mozilla has pointed to[28] the dangers of centralized (or centrally-linked) infrastructure storing sensitive personal information, including biometrics. As several recent large-scale data breaches testify, centralized systems present a single point of failure for malicious attacks. A related issue is the centralization of authentication records which can amplify the surveillance capability of those entities that have visibility into the records. In the case of government IDs, this amplifies the fear of "function-creep" where authentication records can be used for surveillance purposes not contemplated by individuals enrolled in the system. Sensitive personal data provided on the assumption of access to benefits, for example, may be used to harm individuals and interfere with privacy, without options to

opt out or even receive notice.

Alternative technical models that try and address these concerns are emerging. The idea is to design systems where individuals have control over where the identity attributes are used, and with whom they are shared. The focus is to ensure that there is no one centralized data trail of the services to which a user is authenticating.

British Columbia's recent "Services Card"[29] offers an example of privacy safeguards built in to the technical design of an ID system. The system is designed to make the same "card" presented by the resident appear differently in different systems. For example, in the healthcare context it presents as their Health System ID; and in the context of a traffic stop it presents the drivers license number, and has strict data minimization and storage limitation policies in place for authentication logs.

Many of the other emerging models use decentralized, cryptography-based models to ensure that verification of credentials is done by the party with whom the individual shares the credential and there is no one centralized record. Some examples in the private sector include Evernym, uPort[30],

British Columbia's recent "Services Card" offers an example of privacy safeguards built in to the technical design of an ID system. The system is designed to make the same "card" presented by the resident appear differently in different systems.

VeresOne. Governments too are actively funding and experimenting with decentralized systems, for example, Canada.[31] The open standard[32] called a Decentralized Identifier (DID) is controlled by the individual (resident). Any issuing authority, including government agencies can use this identifier to issue a verifiable credential to the resident including travel documents, drivers licenses, and educational credentials. While these models show promise, high levels of complexity and questions around usability and feasibility in their implementation remains a major challenge, especially in the context of developing countries with infrastructural and literacy barriers. There is work to be done to see how decentralized and secure systems can be designed such that they do not rely on high levels of digital literacy to be trustworthy.

2.3 OPEN AS IN ACCOUNTABLE

A CLOSED SYSTEM is one unresponsive to the people and lives it impacts. Centralized designs for National ID systems inherently equip the government and other entities with great power over those enrolled and identifiable by them. This is why the design of these systems must ensure that they remain responsive and accountable to the people whose lives they impact. Openness in several key points of the system is critical to keeping the state's power in check and empowering users to manage how they identify themselves to government and private systems with their awareness and consent. The proactive assertion of identity credentials might be understood in contrast to passive systems like those, for example, that can identify individuals in a crowd using facial recognition algorithms and are designed to evade meaningful consent.

LEGAL ACCOUNTABILITY

One such accountability structure is through laws which regulate information flows of identity information collected by identity systems. These laws must be backed up by credible enforcement mechanisms that apply to the government as well as private entities that are able to access data through this system. A

comprehensive data protection law and regulation of surveillance would go a long way to ensure that the data collected for any ID system is minimal (collection limitation principle) and that the resulting database is not used for purposes outside its main function (purpose limitation principle).

A common concern with ID systems is “function creep” where the ID database is used for an entirely different purpose from what was intended (and often, the basis of which consent was collected). Within western democracies the concern about function creep and data sharing relative to national ID systems came to the fore when large scale mainframe databases began to be implemented across a range of government services[33]. During the late 1960’s and early 1970’s through a whole range of public discussion including articles in mainstream publications[34], government hearings, reports[35] legislative action[36] severely limited the use of the social security number,[37] the de facto national ID in the United States.

Hypothetically, we can imagine a biometric ID that collects fingerprints to prevent fraud in welfare payments. What if that same fingerprint database is later scanned

A comprehensive data protection law and regulation of surveillance would go a long way to ensure that the data collected for any ID system is minimal (collection limitation principle) and that the resulting database is not used for purposes outside its main function (purpose limitation principle).

for matches against crime scene evidence? This use, which potentially turns every citizen into a criminal suspect, could not have been contemplated by individuals when they consented to providing their fingerprints. A robust data protection law that applies to state agencies and law enforcement would prevent this kind of overreach.

A data protection framework would also ensure that once such data is no longer necessary, like if the person opts out or is deceased, then their data is deleted from the system, and that authentication records are retained only for the minimum duration required, if at all. Importantly, a data protection law, similar to the European Union's General Data Protection Regulation, would offer individuals several rights to access their data. In Estonia[38], which has a national identity system, individuals can request access to what information about them is held by each government agency and demand explanations for why. Estonians can generally check who has accessed their data and when, and unauthorized government requests are punishable.

It isn't enough for these legal frameworks to come as an afterthought. Countries that deploy biometric ID systems must have both data protection laws as well as a strong, independent regulator before implementing these systems. Without legal safeguards, the process of data collection for enrolment and authentication (and the consent acquired, if any) is unaccountable and leaves those already enrolled with few options or meaningful protections.

TECHNICAL ACCOUNTABILITY

Technical mechanisms for accountability are also critical. This begins with the underlying design of the overall system and its component parts. Openness during the design phase of these systems is critical to get civil society input to ensure the identity system works in a way that minimizes the risk of harm. Once the system is designed and built it is critical to have technical auditability of the system by independent oversight bodies. It is essential to allow for independent external auditors to review the system's security design and practices along with the ongoing operations. This is even

more true when the code itself is not open sourced.

Another way to achieve openness is to have insight into the actual code of the ID system. Open sourcing code can also give citizens, civil society, companies, and other stakeholders greater confidence in the system and the government's intentions. Making code and associated APIs publicly available allows anyone to audit and verify the security and privacy of the system, and would make visible many potential nefarious activities. Open sourcing an ID system could also create a community of people who are committed to defending the security of the system and building new features that provide greater privacy and control for residents. This is especially true for large scale government systems that interface with society at large, where transparency in the code and related components can mitigate the trust deficit that is inevitable when managing a sensitive database at this scale. Initiatives like MOSIP[39] (Modular Open Source Identity Platform) are also a powerful reminder that open code is not enough. It will be critical to see if governments who adopt this foundation maintain this commitment to openness — both in terms of the code but equally in

It will be critical to see if governments who adopt this foundation maintain this commitment to openness — both in terms of the code but equally in the social and legal systems that will regulate these systems.

the social and legal systems that will regulate these systems.

In the case of India's Aadhaar, Mozilla repeatedly[40] warned that the opaque security practices combined with repeated reports of demographic data being compromised, has made it difficult to trust the reliability of the system. Glaring security loopholes, like the reports[41] that it is possible to purchase editing rights to the Aadhaar database for a paltry sum, are unacceptable risks for a system at this scale. A potential security breach, in this case, would affect more than a billion Indians and put access to several vital public and private services at risk. The continued reluctance to engage an independent security audit of Aadhaar is of serious concern.

This also serves to highlight the gap between ID systems which have an open API and meaningfully open systems. While Aadhaar has an open API and allowed for the development of myriad private and public sector applications, this itself did not ensure much needed accountability in the Aadhaar. In fact, the creation of private ecosystems on top of state-issued credentials must be critically examined, particularly for applications that use personal data in predatory ways (for example, loan creditworthiness). These uses may easily transform an ID system meant to empower into one that is exploitative of citizens.

2.4 OPEN AS IN INCLUSIVE

OPENNESS IS OFTEN KEY to ensuring inclusivity. Inclusive systems are those that allow individuals the ability to participate in technical systems *on their own terms*. At one level, this is the objective of ensuring no one is excluded from an ID system because of physical, social, or economic disadvantage. Given the deployment of these systems in developing countries with low levels of connectivity infrastructure and digital literacy, this is a key concern. A fully card-less system for real time authentication, for example, would be highly unreliable in any context with patchy connectivity or regular electricity outages. These are reminders that in the hurry to "leapfrog" to digital technologies, we must not forget the many efficien-

cies that physical offline systems can provide in particular contexts.

Several existing ID principles speak to this objective of leaving no person behind on account of demographic characteristics or physical characteristics (e.g., people with fingerprints that are worn down by manual labor). However, inclusivity demands that we must place equal emphasis on ensuring that individuals are not denied essential services simply because they lack that particular ID or because the system didn't work; as well as ensuring individuals have the ability to opt out of certain uses of their ID.

The ability to opt out of some uses of unique national identifier numbers is critical especially for those most marginalized in society who might risk the most through profiling. The ability to restrict the sharing of information across contexts becomes crucial for these communities. Take Kenya, where the recent announcement to include DNA data in the ID system has raised serious concerns of the linkages of DNA to ethnic identity. In light of Kenya's history of politicization of ethnic identity[42], the creation of databases with this information is feared to reproduce and exacerbate patterns of discrimination. In India, too, there were concerns with requiring Aadhaar for access to HIV treatment.[43] For these communities, the risk of a record being maintained and potentially being shared in unauthorized ways may have been too big to bear.

2.5 OPEN AS IN TRANSPARENT AND PARTICIPATORY

ID SYSTEMS INVOLVE a range of technical and policy choices, many of which have serious implications on individual rights, security, and public trust. This requires broad ranging consultation, including with technical experts and affected communities, especially at the critical design stage. Yet in reality, many such projects have seen a lack of public consultation, often evading or bypassing mandates for public and Parliamentary consultations. In Kenya, the National Integrated Identity Management System (NIIMS) -- which allows the government to collect several biometrics including DNA -- was passed as an amendment buried in a much larger bill, a clear violation of the

Kenyan Constitution's requirement for public particiation and consultation on substantive legislation. When India finally saw a legislative framework to govern Aadhaar, which was established and operated for 5 years via executive orders, there was controversy because it passed[44] as a "money bill", a truncated process that bypassed the regular parliamentary process of debate and discussion.

This is worrying, as it demonstrates that governments are keen to present ID systems as technical systems that can be passed as executive decrees. It is notable that multiple biometric ID systems in developed countries like the UK, France, and Australia were halted before their implementation after fierce opposition at the consultation phase. This emphasizes the importance of transparency and notice at the design stage of these projects, allowing the public to weigh in on the question of *if* and not just how to implement these systems.

The involvement of many private vendors, often foreign companies, in these technical systems also raises serious national security and privacy concerns given the sensitive nature of the personal data involved. Transparency in vendor procurement is therefore another important aspect of any robust consultation process. For example, the involvement of French vendor IDEMIA, formerly known as OTO morpho in Kenya, also provided biometric voter identification systems during the contested 2017 Kenyan presidential elections, where serious concerns[45] were raised regarding the sale of voter data. Allegations[46] of foreign vendors in Aadhaar (only uncovered through access to information requests) have created public distrust due to the non-transparency with which these contracts were concluded.

A positive example of open and participatory processes around the creation of identity systems with digital components comes from the Canadian province of British Columbia. Before the roll out of its Citizen Services Card, the government actively engaged with citizens via an expert forum,[47] a user-panel,[48] and an online survey available to any resident to share their thoughts. Once they received these inputs, the government then responded to what they heard and learned[49].

3.
RECOMMENDATIONS AND POLICY GUARDRAILS
FOR OPEN NATIONAL IDENTITY SYSTEMS

NATIONAL ID SYSTEMS present a set of technical and policy choices to governments when it comes to their design, implementation, and operation. We hope the following recommendations will guide governments and other organizations toward more open, accountable, and inclusive national ID systems:

- The collection and use of biometrics in any identity system comes with significant privacy risks and should be carefully considered in an open, consultative, and evidence-based process. Experience from various countries has shown that the so-called efficiencies associated with the use of biometrics will vary entirely with the context in which they are deployed and factors such as infrastructure, connectivity, occupation, and digital literacy. Moreover, the institutional, social, and political histories of identification in a country must be considered when deciding to deploy technologies that can be weaponized in the future.

- A multiplicity of choices should be available to people to support the sharing of key identity attributes, rather than the imposition of a single and rigid ID system for all purposes.

The consequences of insisting on a single ID can be dire. As the experiences in both Peru and India demonstrate, not having a particular ID or failure of authentication via that ID can lead to denial of essential services or welfare for the most vulnerable. We should be careful to emphasize the centrality of choices and the absence of coercion as we debate better, and worse, forms of digital identity.

- Digital IDs should be designed from their inception to prevent their use as a tool to enable and amplify government and private surveillance. Countries should critically examine whether logging of authentication requests is needed at all, and should certainly put into place laws to limit the retention, accessing, and sharing of authentication records.The use of national ID numbers retained in the databases of private companies can be used to profile citizens and this usage must be publicly debated and regulated. The ability to cross-link databases through the use of the ID credentials can significantly enhance the tracking capabilities of private companies and should be prohibited or at a minimum governed by law. The creation of private ecosystems on top of government IDs (particularly those with open APIs) must be closely scrutinized, particularly for applications that use personal data in predatory ways, as they may easily transform an ID system meant to empower into one that is exploitative of its users. Such ecosystems must be subject to heightened legal standards of liability and public accountability.

- Data protection laws should be in force, with a strong, independent regulator, before the roll out of any national biometric ID project. These legal frameworks cannot come as an afterthought and must be in place before the roll out of a national biometric ID project.

- ID systems must also be technically auditable by independent external bodies to ensure trust, security, and inclusion. In particular,audits should be conducted to ensure that the ID system complies technically with the legal frameworks

governing the system and personal data. National ID systems that leverage open source code provide an additional layer of transparency and inherent accountability. In general, while an open API design (like that of India's Aadhaar) is welcome in terms of benefits of interoperability across uses, this technical feature does not ensure accountability and trust in the system overall. We recommend all national ID systems should be open sourced.

- Verifiable inclusion should be a core pillar in the design of digital ID systems, where the relevant entities should be held accountable for a breach of the principle. For example, no one should be excluded based on demographic or physical characteristics. Identity systems must account for digital literacy levels of populations and must be resilient in the face of low connectivity environments. Individuals must not be denied essential services because they don't have a particular ID or the system did not function. This would ideally be accomplished by having the freedom to utilise an alternative non-digital ID.

- Individuals must have the ability to opt out of certain kinds of data sharing when using their IDs, especially around sensitive information that might cause harm if disclosed.

- Governments must conduct wide ranging consultation on the technical, legal, and policy choices involved in the ID systems from the design stage of the project. It is notable that multiple biometric ID systems in developed countries like the UK, France, and Australia were stopped before their implementation after fierce opposition at the consultation phase. This emphasizes the importance of transparency and notice at the design stage of these projects, allowing the public to weigh in on the question of *if* and not just how to implement these systems. Consultation with external experts and affected communities must include:
    - input in the design and scoping phase to understand how it will be used, including evaluating concerns

around the use of the system by marginalized and at risk communities;
- ▷ feedback on the legal and policy frameworks that apply to the system;
- ▷ transparency into the procurement requirements and the process through which those procurements will happen;
- ▷ disclosure of the vendors ultimately chosen to implement ID projects given the sensitivity of personal data involved; and
- ▷ heightened public accountability obligations regarding inclusion, especially on the introduction of new features or use cases.

While identity systems can be empowering, they also have incredible potential for abuse, whether in the form of unchecked surveillance, detailed profiling, social exclusion, denial of benefits, and in some tragic cases, even death. A series of technical and policy choices in the design of a digital identity system determine whether the system will be empowering or exploitative and exclusionary. While several organizations have published principles around digital identity, too often they don't act as a meaningful constraint on the relentless push to expand digital identity around the world. Openness provides a useful framework to guide and critique these choices, and to ensure that identity systems put people first.

ENDNOTES

1 Aadhaar Seeding Fiasco: How To Geo-Locate By Caste and Religion In Andhra Pradesh With One Click, Aman Sethi, Huffington Post India, 25 April 2018. Available at: https://www.huffingtonpost.in/2018/04/25/aadhaar-seeding-fiasco-how-to-geo-locate-every-minority-family-in-ap-with-one-click_a_23419643/

2 Vélez, Alejandro. "Insecure Identities. The Approval of a Biometric ID Card in Mexico." Surveillance & Society 10.1 (2012): 42-50.

3 Nadra-linked criminal database becomes operational, Munawer Azeem, Dawn, 29 July 2016. Available at: https://www.dawn.com/news/1273886

4 Government Defends Move To Make Aadhaar Mandatory For Mobile SIM Cards, Arpan Chaturvedi, BloombergQuint, 3 May 2018. Available at: https://www.bloombergquint.com/aadhaar/government-defends-move-to-make-aadhaar-mandatory-for-mobile-sim-cards

5 How private companies are using Aadhaar to try to deliver better services (but there's a catch), M Rajshekhar, The Wire, 22 December 2016. Available at: https://scroll.in/article/823274/how-private-companies-are-using-aadhaar-to-deliver-better-services-but-theres-a-catch

6 Why do you need Aadhaar to investigate a lost package?, Rachita Taneja, Mozilla Blog. Available at: https://blog.mozilla.org/netpolicy/2017/11/16/need-aadhaar-to-investigate-lost-package/

7 Justice K. S. Puttaswamy v Union of India - WP (C) 494/2012, Supreme Court of India. Available at: https://main.sci.gov.in/supreme-court/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

8 Identification for Development Strategic Framework, World Bank, January 25, 2016. Available at: http://pubdocs.worldbank.org/en/179901454620206363/Jan-2016-ID4D-Strategic-Roadmap.pdf

9 Identification for Development (ID4D), World Bank. Available at: https://id4d.worldbank.org/

10 Lyon, David. Identifying citizens: ID cards as surveillance. Polity, 2009.

11 It should be noted that in these countries the "photograph" a form of biometric has been part of identity documents like drivers licenses issued by the state for 50 years.

12 National Identification Cards: Why Does the ACLU Oppose a National I.D. System?, American Civil Liberties Union (ACLU). Available at: https://www.aclu.org/other/national-identification-cards-why-does-aclu-oppose-national-id-system

13 Success Story: Dismantling UK's Biometric ID Database, Electronic Frontier Foundation (EFF). Available at: https://www.eff.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database

14 National ID Cards, Canadian Internet Policy and Public Interest Clinic (CIPPIC), Available at: https://cippic.ca/en/national-id-cards

15 Biometric ID database found unconstitutional, European Digital Rights (EDRi). Available at: https://edri.org/edrigramnumber10-6french-biometric-database-unconstitutional/

16 Biometrics project scrapped after massive delays and budget blowouts, Matthew Doran, ABC News, 15 June 2018. Available at: https://www.abc.net.au/news/2018-06-15/biometrics-project-scrapped-after-delays-and-budget-blowouts/9876068

17 National digital identity programmes: what's next?, Access Now, 21 March 2018. Available at: https://www.accessnow.org/national-digital-identity-programmes-whats-next/

18 The Nail Finds a Hammer: Self-Sovereign Identity, Design Principles, and Property Rights in the Developing World; Michael Graglia, Christopher Mellon, Tim Robustelli. Available at: https://www.newamerica.org/future-property-rights/reports/nail-finds-hammer/

19 ID4D Principles, World Bank. Available at: https://id4d.worldbank.org/principles

20 Identity in a Digital World: A new chapter in the social contract, World Economic Forum. Available at: https://www.weforum.org/reports/identity-in-a-digital-world-a-new-chapter-in-the-social-contract

21 See Note 17

22 The Laws of Identity, Kim Cameron, May 2005. Available at: https://www.identityblog.com/?p=352

23 The Path to Self-Sovereign Identity, Christopher Allen, 25 April 2016. Available at: https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

24 See World Bank ID4D principles, Kim Cameron's Laws of Identity.

25 Vendor lock-in means there is only one vendor whose IDs work within the system and the government must exclusively source from that vendor going forward.

26 Reuben, William, and Flávia Carbonari. "Identification as a national priority: the unique case of Peru." Center for Global Development Working Paper 454 (2017).

27 For India's poorest, an Aadhaar card can be the difference between life and death, Mayank Bhardwaj, Reuters, 12 September 2018. Available at: https://in.reuters.com/article/india-election-starvation/for-indias-poorest-an-aadhaar-card-can-be-the-difference-between-life-and-death-idINKCN1LS0HO

28 Mozilla Statement on Recent Reports of Aadhaar Data Being Breached (again), Jochai Ben-Avie, 1 May 2018. Available at: https://blog.mozilla.org/netpolicy/2018/05/01/mozilla-statement-on-recent-reports-of-aadhaar-data-being-breached-again/

29 BC's Citizen Engagement: A Model for Future Programs, Kaliya "Identity Woman" Hamlin, re:ID, Spring 2017. Available at: https://identitywoman.net/wp-content/uploads/2011/09/reid_spring_14-BC.pdf

30 See Note 18

31 The Canadian Provincial Government work includes British Columbia which has the VonX project http://www.vonx.io and the Alberta Government Credential Ecosystem https://www.aceprogram.ca.

32 Currently being standardized at the W3C. See https://github.com/w3c-ccg/did-wg-charter for more information on formation of the Decentralized Identifier Working Group. The Verifiable Credential's Working Group has been working for 2 years and progressed to a candidate recommendation: https://www.w3.org/2017/vc/WG/

33 See Sarah Igo, the Known Citizen: A history of Privacy in Modern America, 2018

34 See cover story on The Atlantic in November 1967 was The National Data Bank; News Week Cover Is Privacy Dead, July 1970

35 Social Security Number Task Force, Social Security Administration, Report to the Commissioner (1971), Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems July, 1973.

36 U.S. Department of Justice, United States Department of Justice Overview of the Privacy Act 1974, 2015 Edition, E-Government Act of 2002 (Pub.L. 107–347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

37 Chapter 16: The Social Security Number. Personal Privacy in an Information Society, The Report of The Privacy Protection Study Commission, Personal Privacy in an Information Society, The Report of The Privacy Protection Study Commission, July 1977

38 'Government as a data model' What I learned in Estonia, Peter Herlihy, 31 October 2013. Available at: https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/

39 Modular Open Source Identity Platform (MOSIP). Available at: https://www.mosip.io/

40 See Note 28

41 UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm - Rachna Khaira, Aman Sethi and Gopal Sathe, Huffington Post India, 11 September 2018. Available at: https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/

42 Ethnicity and Politicization In Kenya (2018), Kenya Human Rights Commission. Available at: https://www.khrc.or.ke/publications/183-ethnicity-and-politicization-in-kenya/file.html

43 Why Aadhaar is prompting HIV positive people to drop out of treatment programmes across India, Menaka Rao, Scroll, 17 November 2017. Available at: https://scroll.in/pulse/857656/across-india-hiv-positive-people-drop-out-of-treatment-programmes-as-centres-insist-on-aadhaar

44 SC upholds Aadhaar as Money Bill: Here is what experts, govt said back then, Business Standard, 26 September 2018. Available at: https://www.business-standard.com/article/current-affairs/sc-upholds-aadhaar-as-money-bill-here-is-what-experts-govt-said-back-then-118092600734_1.html

45 Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process, The Centre for Intellectual Property and Information Technology Law; Dr. Robert Muthuri, Francis Monyango and Wanjiku Karanja. Available at: https://www.cipit.org/images/downloads/CIPIT-Elections-and-Biometrics-Report.pdf

46 Did UIDAI share biometric data with its foreign vendors?, Sahil Makkar, Business Standard, 30 August 2017. Available at: https://www.business-standard.com/article/economy-policy/did-uidai-share-biometric-data-with-its-foreign-vendors-117083000682_1.html

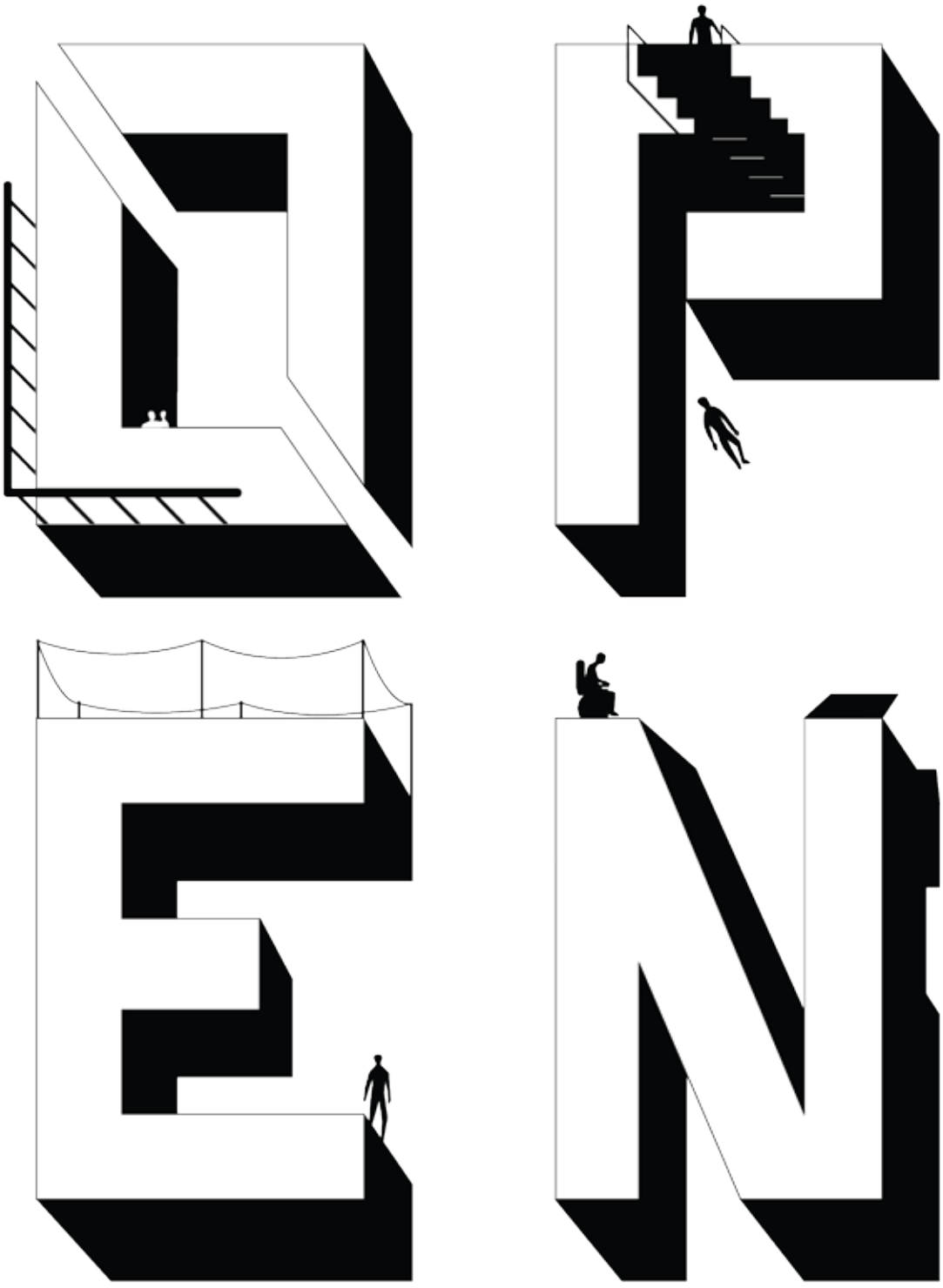
47 See Appendix 1 Identity North Specialist Forum Proceedings https://engage.gov.bc.ca/app/uploads/sites/121/2017/02/Appendix-I-Specialist-Forum-Report-v0225.pdf

48 Recommendation from the BC Services Card User-Panel. Final Report

| December 2013 Prepared for the Ministry of Technology, Innovation and Citizens' Services https://engage.gov.bc.ca/app/uploads/sites/121/2017/02/Appendix-II-Recommendations-from-BC-Services-Card-User-Panel.pdf

49 Digital Services Consultation Fall 2013, Ministers Response. British Columbia Ministry of Technology and Citizen Services, Published March 2014 https://engage.gov.bc.ca/app/uploads/sites/121/2017/02/DigitalServicesConsultation_report.pdf

OPEN AS IN **A MULTIPLICITY OF CHOICES**
OPEN AS IN **DECENTRALIZED**
OPEN AS IN **ACCOUNTABLE**
OPEN AS IN **INCLUSIVE**
OPEN AS IN **TRANSPARENT AND PARTICIPATORY**



moz://a