The Appropriate Use of Digital Identity

A THREE-REGION RESEARCH ALLIANCE

ITS Instituto de Tecnologia & Sociedade do Rio

CIPIT CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW

THE CENTRE FOR Internet & Society

SUPPORTED BY

ON OMIDYAR NETWORK

The Appropriate Use of Digital Identity

THE CENTRE FOR INTERNET AND SOCIETY (CIS), INDIA

Towards a framework for evaluation of Digital ID

16.9 By 2030, provide legal identity for all, including birth registration

UN SUSTAINABLE DEVELOPMENT GOAL

As governments across the globe implement new, foundational, digital identification systems (“**Digital ID**”), or modernize existing ID programs, there is dire need for greater research and discussion about appropriate uses of Digital ID systems. This significant momentum for creating Digital ID in several parts of the world has been accompanied with concerns about the privacy and exclusion harms of a state issued Digital ID system, resulting in campaigns and litigations in countries such as UK, India, Kenya, and Jamaica. Given the very large range of considerations required to evaluate Digital ID projects, it is necessary to think of evaluation frameworks that can be used for this purpose.

What follows is an attempt to build draft principles against which Digital ID may be evaluated. We hope that these draft principles can evolve into a set of best practices that can be used by policymakers when they create and implement Digital ID systems, provide guidance to civil society examinations of Digital ID and highlight questions for further research on the subject. We have drawn from approaches used in documents such as the *necessary and proportionate principles*, the *OECD privacy guidelines* and scholarship on harms based approaches.

When we refer to the ‘use’ of ID below, we mean the use of digital ID to identify or authenticate ID holders, or make authorisations of any kind on their behalf.

Rule of Law Tests

The rise of Digital ID, and the opportunities they present, both for public and private actors, has often resulted in hasteful implementations and adoptions. This does not allow for sufficient deliberation to lead to governance mechanisms. Below are the most *basic tests* to ensure that a rule of law framework exists to govern the use of ID —

1.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law?

Digital ID, by its nature, will entail greater collection of personally identifiable information, as well as privacy risks. Any such restrictions to fundamental rights must be prescribed by law in the form of a publicly available legislative act. Other forms of regulation, such as executive ordinance, only meet this requirement in limited ways.

1.2 DEFINING ACTORS AND PURPOSES

Does the law clearly specify the actors and the purposes?

The law must clearly specify the actors, or a category of actors who may use the Digital ID. Actors include entities who may use the Digital ID, as well as agencies and databases to whom the it may be connected in any way. Similarly, the purposes for which the Digital ID is used, while may not be expressly defined, must always be clearly backed by law.

1.3 LEGITIMATE AIM

Are all purposes flowing from a 'legitimate aim' identified in the valid law?

All the purposes for use of Digital ID must correspond to a legitimate aim identified in the valid law. This legitimate aim must be "necessary in a democratic society," and not based merely on political expediency.

1.4 REDRESSAL MECHANISM

Does the law provide for adequate redressal mechanisms against actors who use the Digital ID and govern its use?

Adequate redressal mechanisms would necessarily include the following three requirements: a) *User Notification*: individuals must be notified when their Digital ID is used in any way; b) *Access and Correction*: individuals must have access to personally identifiable information collected through the use of Digital ID, and the ability to seek corrections, amendments, or deletion of such information where it is inaccurate; c) *Due Process*: individuals must be entitled entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial judicial authority, established by law in cases where provisions of law governing the Digital ID are violated.

1.5 PURPOSES

If legitimate aims for Digital ID correspond to its specific purposes, does the project restrict itself to the uses which directly relate to such purposes?

Once the law or its supporting documents specify the legitimate aims of the Digital ID, all purposes must flow from this 'aim', and all uses of the Digital ID must have a rational nexus to these purposes.

1.6 MISSION CREEP

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in use of Digital ID?

In cases where there is an attempt to use the Digital ID for newer purposes, the executive authority must not be able to allow for such uses in the absence of a legislative process for deliberating the additional uses, or their judicial examination against the legitimate aims.

Rights based Tests

The most clear and outright critiques of Digital ID systems have come in light of their violations of the right to privacy. Across jurisdictions, critics have discussed different forms of violations of privacy, including mandatory collection of sensitive personal data such as biometrics, lack of robust access-control mechanisms, inadequate protection of private sector collection of data, and increased behavioral profiling through use of one identifier for all services. Alongside, there have also been serious questions raised about exclusion concerns where absence of an ID or failures in its functioning can lead to denial of basic entitlements and benefits. Key rights-based principles are highlighted below —

2.1 NECESSARY AND PROPORTIONATE PRIVACY VIOLATIONS

Are the privacy violations arising from the use of Digital ID necessary and proportionate to achieve the legitimate aim?

The use of Digital ID may pose inherent risks to the right to privacy by leading to generation of more data, facilitating the connection of varied sets of behavioral data to unique identities, and involving a set of actors. Privacy violations arising from the use of Digital ID must satisfy the requirement of being necessary for achieving the legitimate aim. This means it must be the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon the privacy rights. Additionally, the privacy violations caused by the use of Digital ID must be proportionate to the legitimate aim being pursued.

2.2 ACCESS CONTROL

Are there protections in place to limit access to the digital trail of personally identifiable information created through use of Digital ID by both state and private actors?

Privacy risks to individuals from use of Digital ID arise both from generation of data, as well as access to the generated data. Therefore, adequate access control mechanisms would entail access to information generated as a result of the use of Digital ID would be limited to actors who need this information to achieve specified purposes.

2.3 EXCLUSIONS

Are there adequate mechanisms to ensure that the adoption of Digital ID does not lead to exclusion or restriction of access to entitlements or services?

If the intended use of ID could lead to denial or restriction of services or benefits to individuals, or categories of individuals, then there must be mechanism to ensure that such individuals are not disadvantaged. In these cases, individuals must be able to use other forms of identification to seek access to services or benefits.

2.4 MANDATORY USE

In case enrolment and use of Digital ID are made mandatory, are there any valid legal grounds for doing so?

Whether enrolling into and specific uses of ID should be mandatory or not remains one of the most important questions in ID. As mandating ID limits the agency of individuals, it should be subject to strict legal tests, such as the need to obtain information that is strictly necessary to provide a service to an individual, prevention of harm to others, and eligibility to undertake specialised tasks.

Risk based Tests

The debate and discussion around Digital ID has centered primarily on the perceived or existing risks related to privacy, welfare, equality and inclusion. As a range of use cases of Digital ID emerge, laws and institutions governing Digital ID must be vigilant about the risks and harms emerging from them. This needs to be done with some urgency regarding the existing use cases of Digital ID, as well. A rights based approach is, by itself not sufficient to address these challenges, and there is a need for greater paternalistic regulatory measures that strictly govern the nature of uses of Digital ID. Below we attempt to articulate some draft principles. These principles do not exist in most jurisdiction dealing with Digital ID, though there is now an increasing focus on harms assessment in prominent frameworks such as the GDPR.

3.1 RISK ASSESSMENT

Are decisions regarding the legitimacy of uses, benefits of using Digital ID and their impact on individual rights informed by risk assessment?

Drawing from consumer protection laws, laws governing Digital ID need to take into account tangible harms to individuals, have clear provisions on prevention, and for appropriate recovery for those harms, if they occur.

3.2 PROPORTIONALITY

Does the laws on Digital ID envisage governance, which is proportional to the likelihood and severity of the possible risks of its use?

Regulation of Digital ID needs to be sensitive to the actual harms caused by its uses, and be informed by the severity and likelihood of harm. For instance, a design involving the centralised storage of biometric data with robust security safeguards may have a remote likelihood of security risk, but has a very high severity in cases of breach.

3.3 RESPONSE TO RISKS

In cases of demonstrable high risk from uses of Digital ID, are there mechanisms in place to prohibit or restrict the use?

If the risks from uses of Digital ID are demonstrably high, they need to be restricted until there are adequate mitigating factors that can be introduced. This may need a responsive Digital ID regulator, who has the mandate and resources to intervene responsively.

3.4 DIFFERENTIATED APPROACHES TO RISKS

Do the laws and regulations envisage a differentiated approach to governing uses of Digital ID, based on the likelihood and severity of risk?

Drawing from Fred Cate's model of harms in data protection, a differentiated approach may involve categorising uses as (a) *Per Se Harmful*: where a use is always harmful (e.g., the use of ID to collect and use alternative data proven to be predatory for credit scoring and lending), the regulator could prohibit the use outright; (b) *Per Se Not Harmful*: the regulator may consider not regulating uses that present no reasonable likelihood of harm; and (c) *Sensitive Uses*: where use of personal data is neither *per se harmful* nor *per se not harmful*, the regulator may condition the use on several factors, such as aligning with a rights based approach.

INSTITUTE FOR TECHNOLOGY & SOCIETY (ITS), BRAZIL

When should digital identities (not) be used?

For digital identity regimes to be effective, considerations must be made for the edge use cases and exceptions, in order to be truly universal and ubiquitous

WORLD ECONOMIC FORUM, 2018

Digital identities (DIDs) represent the milieu of socio-technical systems - on one hand, they enable individuals to enjoy digital services and on the other, serve as the basic infrastructure of modern states and prominent industries. DIDs have the power to facilitate both top-down and bottom-up development, giving citizens the power to take charge of their digital lives and states, the tools for multi-level governance, simultaneously. How does one then design, implement and manage DIDs so as to realize the aforementioned benefits? And moreover, what are the preconditions for properly using DIDs? In this document we highlight some of these aspects and considered the value-add one as the umbrella for analysis. A framework adapted from existing ones and focused on policy tradeoffs will be developed in the following stage. In parallel, a series of interviews and online meetings with CSOs stakeholders of Latin America to validate and adjust the framework assessment of policy tradeoffs will be conducted.

When do DIDs may add value? How can we define this methodologically and strategically?

A traditional way of thinking about value-add could be in terms of value-add to the economy. A recent McKinsey report (2019) states that Brazil's GDP may increase up to 13% due to a DID system. However, we propose to rethink the concept of value-add - if the use of DIDs demand a defined value-add, one must think of value as more than financial benefits. For instance, how do DIDs increase the level of political engagement in and impact on local governance? A way of addressing this issue perhaps, is by assessing utility both qualitatively and quantitatively at the user level - for instance, how do DIDs bring about cost or time savings to the user. We will map and illustrate the major use cases in which the value-add is significant. These aspects are also directly related to the interoperability level of the system in terms of shared databases among multiple entities and standards for cross-border validation.

Some other forms of defining value-add could include fraud reduction, support to local innovation ecosystems, financial inclusion and so on. A report by BCG (2012) argues that two-thirds of the total value of DID may be wasted if there is not “trusted flow of personal data”. Additionally, according to OIX (2018), “cost of doing nothing” also posits implications on future costs and savings. One could also think of value-add in terms of policy trade-offs. Can we assess gains and losses through economic empowerment vs. commoditization of self; public vs. private management; and strong vs. weak system infrastructure? The next step of the research we will address these policy tradeoffs mainly targeting the Latin American context.

Lastly, value also points to the question of demand and supply. Is there a market for identification? Are there ID services being offered? By/for whom? The use of identities is mostly purpose bound. We think that only by identifying needs that can truly be solved through identification can one avoid “mission creep” and add “real value”. Moreover, a recently study from Caribou Digital in Bangladesh has identified some major values a digital ID can add by surveying users. Among them it is worth mentioning: gender inclusion by enabling women remote work; formalizing the economy and thus ensuring safer jobs; having fast and easier access to medical care; or just to proof a citizen status.

How can DID coverage be inclusive rather than exclusive? How do we implement DIDs that do not exclude citizens without access ICT?

The premise of coverage is that it is impossible to identify citizens without reaching them first. One can break coverage further into two layers: 1) *the breadths of citizen identification* - What is a state’s capability to reach all its citizens in the territory? Is there a widespread census program and databases?, and 2) *the depths of citizen identification*. How many data points does a state collect on each of its citizens? Does this identification system include highly sensitive data including biometric data? Which data is required to access what benefits?

Identification infrastructure is a precondition for citizens’ access to the use of DID and its benefits. Lack of coverage could reveal a lack of access to the use of services provided by citizens not covered by the infrastructure. For example, this situation could lead to a differentiation between citizens who have access and those who do not. It is important to assess the extent to which uses of digital identities generate exclusions and how they are related to digital identification itself. Hence, the central issues in relation to this topic is: currently available infrastructure would make it possible for citizens to fully access services offered by digital identities? How the exclusion risk is being assessed in a context? This by assuming that appropriate uses of digital identities have a clear position with this regards in terms of how risks and mitigation strategies.

Institutional components are next in this discussion of coverage - here, governance and interactions between ID providers and users become crucial. We discuss some of these aspects later in this document (what is the optimal level of human, institutional, data and technological interoperability for a digital identity strategy to thrive?).

Lastly, to further the topic of service provision, we think that a measure of inclusiveness is by assessing the reach and impact of DIDs to vulnerable groups or minorities. For those who do not want to have a fully digital identity or only want to share relevant identity data, how does one define coverage?

What levels of digital literacy must the population have? What set of skills are needed to use a digital identity system?

Analogously to the infrastructure conditions digital literacy is a key thread connecting coverage of digital identities and their appropriate uses, which then brings us to the question of appropriate levels of digital literacy to fully enjoy the benefits of digital identities. We assume that the greater the digital literacy, the more appropriate uses there will be. However, before we define an appropriate level of digital literacy, we think that it is important to ‘classify’ a population - whether in terms of residency (rural vs. urban), gender, under-representation, educational levels, income levels, or even by ‘keenness to adopt’. Barriers for enrollment, management and use of digital identities platforms can vary considerably from a territory to another. In the sense, DID strategies and their uses design must take contextual factors at the core.

Looking further, we identify the basic components of digital literacy - most of which, are covered by toolkits that recommend ways to assess levels of digital literacy - include the capacity to browse, to comprehend and of to solve problems. When it comes to DID, these skills elicit the following questions - How do literacy levels then affect participation in digital ID systems? What about the compulsory aspect of adopting digital ID schemes, are the citizens aware of it? Higher participation levels create more intrinsic value-add for the entire DID system, one example are the civically engaged citizens directly voting in projects of law and petitions.

Thirdly, literacy cannot be thought of separate from digital literacy, especially when thinking of the “next billion connected people” - it must only be a successor in this regard. In the absence of literacy, while technologies such as voice recognition can provide inclusion, they also expose populations to vulnerabilities. How does this affect user control? Moreover, how does the user perceive this relative advantage of being identified?

Fourthly, we recognize the digital literacy of the ID providers as another key consideration in implementation strategies. Especially, in the case of the public sector entities, what is their technology capacity? That is, does the state have internal capacity either to develop its own system or to produce comprehensive technical specifications to hire a private party to develop its own system? Linking this back to value-add for DIDs, one can then infer that ‘inappropriate’ levels of digital literacy may increase costs of implementation of DIDs for agencies and states.

Finally, the importance of digital literacy is further exposed when one compares proxy-digital identities such as social media registries and self-asserted distributed ledger wallets as a source of identification. The legality and applicability of these proxy identities also invoke questions of privacy and appropriate usage that states and agencies must take into account when designing DID systems.

Building and maintaining trust in the system: key to the appropriate use of DID

As identified in several DID literature, trust is essential to ensure the adoption and to promote ongoing usage of digital identity by institutions and individuals. Building trust must be conceived as a critical aspect throughout the identity lifecycle for its appropriate use. Nonetheless, according to data from Omidyar Network, majority of interviewed people in 60 countries do not trust their data to governments or private entities. This research and also the one from Inter-American Development Bank show that Latin American citizens are more suspicious of their governments than in other parts of the world, being more likely to trust private entities.

It is appropriate to deploy some factors that influence directly on the trust and, therefore, may culminate in inappropriate uses of DID systems. First, if users do not trust the institutions handling their data (the system provider or requesting parties), they will be reluctant to share their personal information and use that system. Without user there is no value-add. Second, individuals are more or less data-trust sensitive of certain types of data and, therefore, more or less willing to share them. According to the BCG's digital identity survey, the type of data is one of the most important factors in a user's decision to share personal data (being financial and health data the most sensitive ones; and often mentioned as use cases of digital identities).

We believe that trust comes with the quality of the services provided and the corruption perception. Is the system provider ready to assure a service that works properly and continuously, so as not to lose its functionality in the eyes of stakeholders and consequently leads to discontinuation of its use? How does the government assure citizens in a recent past context of authoritarian regime or high levels of perceived corruption? Building and maintaining trust is fundamental to exploiting the full potential of digital technologies in general and their value. Once eroded, it is difficult to be recovered and carries with it the gained value in revenues and efficiency.

The greater the amount of information gathered in a single system, the more uses they are apt but also greater the risk for the user data and privacy (security breaches; exposure of sensitive data, etc) and more likely to Thus, the information collected and the reliability of the institutions should be considered when designing the appropriate system architecture (centralized, federated or decentralized) and in the trade-off between a digital identity that achieves the greatest possible multiple application areas and risks to users' privacy. Good ID builds trust with transparency and accountability. And that is why it is imperative that the implementation of a robust, effective, transparent, comprehensive ID System is well-debated between public and private service providers and citizens.

A straightforward and well-publicized procedure is key to give users clear notion about how and with what purposes their data is captured, handled. What is this ideal framework and communication strategy? It should assure adjudication of grievances, besides authentication and service delivery systems that use a minimal amount of contextualized data to protect user privacy.

Is DID linked to Civil Registration? Does it have a legal framework?

Similar to potential value-add, the legal character of a DID also functions as an umbrella to DID implementation. United Nations adopted the concept of "Legal Identity" to highlight that identification is a dimension of legal personality, not only a biological fact. It means that it does not refer to technological issue as well as there is not such an opposition of "legal vs. digital".

The Asian Development Bank defines legal identity as one that "*... allows persons to enjoy the legal system's protection and to enforce their rights or demand redress for violations by accessing state institutions such as courts and law enforcement agencies*". We assume that Civil Registration is the foundation of the legal dimension, and DID must be be linked to it. However, there are examples of DID that were developed and implemented without legislative enforcements. Aadhaar, in India and, more recently the Huduma Namba registration rallied as mandatory in Kenya, serve as key examples.

In this sense, Is it adequate to label a digital identity as appropriate without it being linked to a civil registration? In which circumstances? Several identification schemes can be developed based on innovative technology (what is happening in the distributed ledger phenomenon, for instance), but to be a Good ID solution, we think that they need to be part of a legal framework. ■

CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW, KENYA

When should ID be used?

QUESTION

When should ID be used?

ANSWER

An ID system should be used when the government is willing to be transparent about the system.

Case Study: The ongoing implementation of NIIMS in Kenya

Abstract

In this non-scientific study, we look at the ongoing implementation of a new ID system in Kenya. By shrouding the development and implementation of the ID system in secrecy, we argue that the government has done itself a disservice, providing fertile ground for the spread of rumors and conspiracy theories. The immediate and most notable result is the pending lawsuit against the system, indicating a lack of buy-in from civil society and other groups. We conclude that transparency at each stage in the process of designing and implementing an ID system is critical, and that government should not pursue a system unless it is willing and able to do so openly.

Background

In a 2019 article, Keith Breckenridge[1] broke down "the recent failure of an elaborate biometric registration scheme, the National Digital Registry System, in Kenya." The NDRS is described as a 2014 plan by the Government of Kenya (GoK) for inclusive biometric registration. The plan ultimately failed, but the process was perfectly illustrative of the tenuous nature of national identification schemes. As Breckenridge observed:

> *The contracts for state identity registration are lucrative sites for international firms' profits, and also, notoriously, for the extraction of rents by local decision makers. These possibilities for rent-seeking and the anticorruption reforms and mechanisms that police them make the ground on which state-funded identification projects develop treacherous indeed. And this is especially true, in Kenya and many other African countries, where the prospects of meaningful democracy – and control over the states' revenues – are determined by the integrity of the identity registration processes.*

Less than five years later, the GoK introduced the National Integrated Information Management System, NIIMS, through a bit of legislative maneuvering. Now colloquially known as Huduma Namba, initial registration for NIIMS occurred in April and May 2019. Simultaneously, various civil society organizations filed lawsuits, seeking to halt the process. The ongoing litigation has marred (but not halted) the initial registration period, as the court made interim orders that registration for NIIMS could not be made compulsory and could not include DNA or GPS data, and that the government cannot deny services to those who do not register.

Observations

A nationwide identification system typically progresses through predictable stages:

> *conceptualization of the system based on identified needs and goals;*
>
> *ensuring a legal framework exists for the conceptualized system;*
>
> *development of the actual system as per the conceptualized system and enabling legal framework;*
>
> *initial rollout and registration of persons covered by the system; and*
>
> *ongoing maintenance of the system.*

Throughout the entire process, implementation of NIIMS has been anomalous.

First, conceptualization of the system appears to be rooted, at least in part, in the final report by a Taskforce appointed in February 2018 by the Ministry for Information, Communications, and Technology to analyze “digital technologies that demonstrate great potential to transform Kenya’s economy”.[2] That final report was announced in November 2018, but since it remains unpublished and unavailable, it is currently impossible to determine whether the implementation of NIIMS has followed the recommendations of the Taskforce.

Second, the legal framework for NIIMS was provided by amendment of the Registration of Persons Act. Specifically, section 9A was added to that Act via the passage of the Statute Law (Miscellaneous Amendment) Act 2018 on 31 December, 2018. Although public participation was allowed, the Miscellaneous Amendment Act 2018 is 86 pages and contains amendments to 52 separate laws. It is not difficult to conclude that the amount of public participation for the NIIMS provision was necessarily less than it would have been had the Registration of Persons Act been amended directly and separately.

Third, the details of the actual implementation of NIIMS remain unclear. It is publicly known that the French company OT/Morpho (now IDEMIA) provided registration kits, that those kits capture data (including biometric data) on removable storage media, and that the process of registration involves uploading data from the removable storage media. It is not publicly known, however, exactly what happens to that data after uploading. This has raised at least the following questions:

> *Where is the data stored (currently and in future), and in what format?*
>
> *What system is in place to ingest and store the data?*
>
> *How will the ID number (the "Huduma Namba") be generated?*
>
> *What safeguards are in place to ensure that the data are secure? Who will have access to the data?*

It does not help the cause of transparency that IDEMIA was recently "blacklisted" and blocked by the Kenyan Parliament from working in Kenya for the next 10 years.[3] The Parliamentary decision cited irregularities in securing tenders and violations of the Companies Act.

Fourth, the registration period (April and May 2019) was peppered with statements from the government that clearly contradicted the spirit, and possibly the letter, of the interim court ruling. Various government officials indicated that mobile phones would be disabled (i.e., SIMs locked), services would be denied, and there would be other, unspecified consequences for non-registration.[4]

Results

In part due to the irregular way in which NIIMS is developing, a number of rumors and conspiracy theories have been circulating:

> *David Ndii proposed that Huduma Namba is a plot by President Kenyatta and his family to take over control of certain aspects of the banking industry.*[5]
>
> *Huduma Namba is a ploy by Mastercard to capture the lending market.*[6]
>
> *Various sources (mentioned by reputable media houses) report that the Huduma Namba is "Demonic".*[7]
>
> *Kenyans living abroad report that they are refusing to register because of the belief that Huduma Namba is a plot by the Kenya Revenue Authority at taxing income earned abroad.*
>
> *Robert Alai, a Kenyan social media influencer, declared that Huduma Namba was a plot by the Chinese to enable "strong surveillance on Kenyan civilians."*[8]

The rumors may range from plausible to absurd, but the pending litigation is a serious threat to the implementation of the system. Notwithstanding the obvious observation that a nationwide ID system that includes biometric and other sensitive data should be implemented in an environment with proper legal protections for data misuse and loss, the lack of information about the system is clearly a driving factor motivating those challenging the system.

Conclusions

We conclude with a seemingly obvious statement: transparency of process matters. ■

Notes

[1] Breckenridge, K., (2019) "The Failure of the 'single source of truth about Kenyans': The NDRS, collateral mysteries and the Safaricom monopoly," *J. African Studies*, 78(1), 91-111.

[2] The Kenya Gazette, 9th March 2018, vol. CXX, no. 33, p. 656.

[3] See, e.g.: *https://www.theeastafrican.co.ke/news/ea/Kenyan-MPs-vote-to-block-French-firm/4552908-5086854-gqxk5x/index.html*

[4] See. e.g.: *https://www.the-star.co.ke/news/2019-05-14-you-will-suffer-without-huduma-namba-state/*

[5] Ndii, D. "Crony Capitalism and State Capture 2: Documents Reveal the Kenyatta Family's Plans to Take over Lending to SMEs" The East African Review, published online 2 April 2019. Link: *https://www.theeastafricanreview.info/op-eds/2019/04/02/crony-capitalism-and-state-capture-2-documents-reveal-the-kenyatta-familys-plans-to-take-over-lending-to-smes/*

[6] See, e.g., *https://citizentv.co.ke/news/kenyans-fault-huduma-namba-plan-over-mastercard-links-right-to-privacy-232187/*. Also see Mastercard Press Release dated 7 February, 2017, "Huduma Card Delivers Cashless Efficiency, Powered by Mastercard Technology". Link: *https://newsroom.mastercard.com/mea/press-releases/huduma-card-delivers-cashless-efficiency-powered-by-mastercard-technology/*

[7] See, e.g., *https://www.standardmedia.co.ke/article/2001319344/is-huduma-namba-the-biblical-666*

[8] See *https://twitter.com/robertalai/status/1098797192356216832*

The Centre for Internet and Society (CIS)

www.cis-india.org
www.digitalid.design

CIS is a non-profit organization, based in India, that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The research at CIS seeks to understand the reconfiguration of social processes and structures through the Internet and digital media technologies, and vice versa. Through its diverse initiatives, CIS explores, intervenes in, and advances contemporary discourse and regulatory practices around internet, technology, and society in India, and elsewhere.

The Institute for Technology & Society (ITS)

www.itsrio.org

ITS is a non-profit organization, based in Brazil, with a mission to ensure that Brazil and other emerging markets respond creatively and appropriately to the opportunities provided by technology in the digital age, and that the potential benefits are broadly shared across society. Through its own research and in partnership with other institutions, ITS Rio analyzes the legal, social, economic, and cultural dimensions of technology and advocates for public policies and private practices that protect privacy, freedom of expression, and access to knowledge.

The Centre for Intellectual Property and Information Technology Law (CIPIT)

www.cipit.org

CIPIT is an academic think tank based at Strathmore Law School in Nairobi, Kenya. Research at CIPIT addresses emerging issues that have continent-wide impact. CIPIT provides an African voice for research networks in emerging markets, ensuring visibility of the local, region, and continental context that is unique to Africa. Ultimately, CIPIT strives to prove that Africa can grow and support a world-class academic research centre in matters of intellectual property and IT law.

SUPPORTED BY OMIDYAR NETWORK

Designed at the *Centre for Internet and Society*, India by Pooja Saxena and Saumyaa Naidu
Printed at P*acific Creative Solutions*, New Delhi