

NATIONAL DIGITAL IDENTITY PROGRAMMES: WHAT'S NEXT?

FINAL DRAFT FOR COMMENT

National Digital Identity Programmes: What's next?

FINAL DRAFT FOR COMMENT | MARCH 2018

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY	2
II. CONTEXT FOR THE NATIONAL DIGITAL ID DEBATE	5
Case Studies	7
<i>Estonia</i>	7
<i>Tunisia</i>	10
<i>India</i>	12
III. TERMS FOR THE NATIONAL DIGITAL ID DEBATE: DEFINITIONS	18
IV. POLICY RECOMMENDATIONS	20
Governance	20
Privacy and Data Protection	22
Cybersecurity	25
V. USE OF BIOMETRIC DATA IN ID SYSTEMS: SPECIAL CONSIDERATIONS	30
VI. CONCLUSION	32

I. EXECUTIVE SUMMARY

Digital identity is increasingly the focus of policy discussions across several different countries, with a number of governments proposing or implementing national digital identity programmes, and multilateral institutions making investments. Through these government-administered or coordinated programmes, governments aim to provide a single digital identity to residents (or sometimes only citizens) of a particular nation state. Many such programmes entail a push to collect, store, and use the biometrics of individuals as the primary means of establishing and authenticating their identity.

Proponents of biometrics linked-national ID programmes argue that they bring benefits such as more accurate and efficient delivery of government services, anti-poverty regimes and welfare schemes; that they can reduce corruption or increase inclusion; or can help serve national security interests. Critics have responded by noting that national digital identity schemes may not in fact ensure more effective distribution of benefits, better service delivery, or improved governance, and at the same time, they raise serious concerns, including concerns about how the programmes are designed or governed; social exclusion; privacy and data protection; and cybersecurity.

As an organisation committed to defending and extending the digital rights of users at risk, Access Now has deep concerns about any initiative to legally mandate a centralised national digital identity programme. These programmes pose significant risks for human rights. Specifically, they threaten to undermine the **right to privacy** and chill **freedom of movement, the freedom of expression**, and other protected rights. Further, since they typically entail the creation of centralised troves of sensitive personal data, susceptible to breach by malicious actors or abuse by public authorities, they also carry risks for **cybersecurity and information disclosure**. When they are biometrically linked and made mandatory, they have the potential to turn a digital ID into a pervasive means of identification, tracking, or control.

It is in this context that we are skeptical, despite the identified benefits of proponents, about the push to universalise national digital identity programmes. From our perspective, it is not helpful for policy makers to advance the idea that identity and civil liberties are necessities that must be balanced against one another; identity must be prefaced on the protection of our civil liberties, not given at the expense of these liberties. Without proper human rights safeguards that are rigorously followed, national identity programmes can be counterproductive to the welfare of the people, violate internationally protected human rights, and undermine our cybersecurity. **If the necessary safeguards are not included in national identity programmes, we recommend that they be arrested and restructured.**

This working paper examines national digital identity programmes from a human rights perspective, discussing the context for the debate about these initiatives globally and proposing safeguards and policy recommendations for those involved: public officials, lawmakers, representatives from judicial and human rights institutions, technologists, officers of development institutions, and members of the private sector. It includes case studies for Estonia, Tunisia, and India, as well as a section that defines terms in the debate. Finally, in a separate section, we discuss special considerations and recommendations related to biometric IDs, whether in government programmes or private sector use.

Following is an overview of our recommendations and digital rights safeguards, which we explore in detail in Section IV. They fall under three pillars:

1. GOVERNANCE

- 1) Ensure a defined and restricted scope of use for the digital ID programme, provided for in the law;
- 2) Make enrollment and use of the digital ID voluntary;
- 3) Create independent and well-designed mechanisms for grievance and redress; and
- 4) Ensure inclusion at the enrollment stage, and no exclusion during implementation, due to technology or infrastructural capacity gaps.

2. DATA PROTECTION AND PRIVACY

- 1) Limit the purpose for which these data are collected and used. Put in place proper measures to prevent user profiling based on the data volunteered;
- 2) Grant individuals rights related to their own data, such as accuracy, recitation, and opt-out;
- 3) Institute robust data protection frameworks to which digital ID programmes are subject;
- 4) Minimise the amount of and type of data governments and associated service providers collect; and
- 5) Restrict lawful interception and monitoring of digital ID use and implement measures for accountability.

3. CYBERSECURITY

- 1) Institute capable foundational technology infrastructure;
- 2) Ensure that data collection and storage are not centralised;
- 3) Separate the functions of identification and authentication and avoid creating transaction logs for authentication;
- 4) Institute "privacy by design" principles in the programme;
- 5) Ensure that national ID programmes are based on models for secure communications, including providing end-to-end encrypted traffic as far as possible.
- 6) Provide transparency in terms of disclosure of cybersecurity policies;
- 7) Provide a legal and policy framework that incentivises reporting and disclosure of vulnerabilities; and
- 8) Take steps to notify affected parties in case of breach of data.

NOTE TO READERS

We welcome all queries and input on this working paper. In particular, we welcome discussion and suggestions on the terminology we use and our policy recommendations regarding national digital ID programmes and the use of biometrics in the public and private sectors.

We aim to release an updated and finalised publication based on this paper in 2018. Please direct your queries or comments to the following Access Now policy team members:

Naman M. Aggarwal (naman@accessnow.org)

Wafa Ben-Hassine (wafa@accessnow.org)

Raman Jit Singh Chima (raman@accessnow.org)

II. CONTEXT FOR THE NATIONAL DIGITAL ID DEBATE

Our primary focus in this paper is national digital identity programmes — that is, policy schemes that governments directly administer or coordinate, which aim to provide a single “digital identity”¹ to residents or citizens of a particular state. These digital identities are often comprised of highly sensitive personal information that serves as the basis of authentication or verification of the person’s identity. In many such proposed or current programmes, governments store this type of information in centralised databases.² That is a mistake.

Mandated identity requirements harm anonymity and place users at risk. As David Kaye, the United Nations special rapporteur on the promotion and protection of the right to freedom of opinion and expression, noted in May 2015, “...encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection”. His report concluded:

“... States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users.”³

Further, centralised troves of personal data are susceptible to breach by malicious actors and abuse by public authorities, by way of access to personal data and government-led or sponsored surveillance and hacking.

Nevertheless, over the past couple of years, several national governments, as well as multilateral institutions, have shown strong interest in national digital identity programmes.

Most recently, in February 2017, the World Bank Group coordinated the creation and release of “Principles on Identification for Sustainable Development: Toward the Digital Age”⁴ through its Identification for Development programme, often referred to as “ID4D”. The ten principles aim to guide governments in the creation and implementation of identification systems. The principles, as well as the annual ID4D report, are set in the context of achieving the United Nations Sustainable Development Goals, specifically target 16.9, which states, “By 2030, provide legal identity for all,

¹ For a fuller understanding of the term “digital identity”, please refer to section III of this paper.

² In this paper, we provide case studies of governments that handle personal information in a centralised manner. We note that others have emphasised that national ID systems can evolve in other ways. For example, Jim Harper at the Cato Institute has indicated that a national ID system has three elements: (1) it is used for identification, (2) it is nationally uniform in its key elements, (3) its possession is either practically or legally required. See Jim Harper, Policy Analysis: The New National ID Systems, Cato Institute, 30 January 2018, Number 831, <https://www.cato.org/publications/policy-analysis/new-national-id-systems>.

³ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, 22 May 2015, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

⁴ The World Bank, Ten Principles on Identification for Sustainable Development, <http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples.pdf>.

including birth registration”. In the report, and subsequent conversations around it, proponents of digital ID programmes often conflate traditional legal identity with digital identity, especially when attempting to persuade lawmakers in countries of the Global South and emerging economies to “leapfrog” traditional paper-based approaches.⁵ Yet governments opting to bypass the primary and foundational steps of creating legal identity programmes by establishing national digital identity programmes instead often introduce issues that threaten users’ rights and the security of their personal information.

Another rationale that proponents of national digital identity programmes advance is that their use is necessary, or foundational, for implementing various international development efforts for economic inclusion and financial technology, sustainable development, and national security.⁶ The need to link national digital identity with the biometric data of the cardholder is attenuated.

While the arguments for legal identity can be convincing — since it can be useful for attaining social benefits and going about regular day-to-day activities that require the verification of identity — those for mandating a national digital identity, including those proposing a link to biometric data, are not. Individuals should not be compelled to put their personal, unchangeable, biometric data at great risk of privacy intrusions for the sole purpose of “proving” legal identity, which can be verified in a variety of different ways. Avoiding this risk is even more important given that national digital identity programmes are often first introduced in communities where people have less reason to trust public authorities, including rural communities and those of marginalised people, such as refugees or other minority groups.

For digital identity to be empowering in certain contexts, the legal and policy framework must be built on a foundation of user agency and choice, informed consent, recognition of multiple forms of identity, the space for anonymity, and respect for privacy. Focusing on one centralised, directly administered national identity system precludes the formation and competitive use of multiple forms of identity — competition that could lead to more efficient and empowering outcomes for users. In fact, some argue that government policy should focus on encouraging the development of a variety of identification and credentialing systems, and instead of insisting on its own particular issued national identity, governments should accept any card or device that provides sufficient proof of the information required for a given transaction.⁷

Further, it is important to remember that given the development of technology, it is far from settled that the best solution for verifying an individual’s identity is national digital identity systems that

⁵ *Id.*, Identification for Development (ID4D), “With the transformational potential of modern solutions—the advances in identification technology (both digital and biometric) and the dramatically falling costs of technology and implementation—there is an opportunity to leapfrog traditional paper-based approaches and build strong and efficient identification systems at a scale not previously achievable,” <http://www.worldbank.org/en/programs/id4d#>.

⁶ *Id.*

⁷ National ID Systems, Chapter 21, Cato Handbook for Policymakers (8th ed., 2017), https://object.cato.org/sites/cato.org/files/serials/files/cato-handbook-policymakers/2017/2/cato-handbook-for-policymakers-8th-edition-21_0.pdf

require centralised, biometric-based authentication. For example, some scholars propose the use of blockchain technologies to authenticate a user's identity. Since the data stored on the public chain is extremely difficult to change, a user need not provide biometric or other types of personal information to authenticate identity. Instead, minimal information about the user is stored on the blockchain, and the identity is verified as valid because of such placement. However, other scholars have warned about the blockchain's potential to violate European privacy law,⁸ specifically the General Data Protection Regulation (GDPR), which holds that under many circumstances, individuals must have the capacity to demand that their personal data be rectified or deleted. This is technically infeasible on the blockchain. It remains to be seen how useful the blockchain can be for digital identity management, but these discussions show that there is more than a single path forward, and some solutions may be considerably less risky, and more effective, than the ones contemplated today.

CASE STUDIES

It is crucial for stakeholders not only to consider the broader issues and concerns raised by a centralised, biometrics-linked approach to national digital identity, but also to learn from the attempts in multiple jurisdictions to develop and implement such programmes. At both a conceptual and practical level, these programmes are raising concerns for privacy, data protection, governance, and cybersecurity. They also raise concerns related to scheme design and the inclusion — or exclusion — of people from government services. We present three country case studies below: Estonia, Tunisia, and India.

Estonia

Estonia is known for pioneering digital governance. Having gained independence in 1991, Estonia, like a true millennial, leverages technology in every aspect of governance. This is the concept behind “e-Estonia”. Estonia is the first nation to hold elections over the internet, and to provide e-residency. The Estonian identity card is another step in the direction of an e-government.

The ID card is a mandatory identity document for citizens of Estonia. It serves the twin function of giving proof of identification and establishing one's identity specifically in the electronic environment, including serving as one's digital signature.

⁸ <https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/>

Under Estonia's Digital Identity Programme, the ID System is leveraged three ways:

ID Card

This card contains the general components of a legal photo ID. However, in addition to the legal photo ID components, a chip on the card carries embedded files, and using 2048-bit public key encryption, it can be used as definitive proof of ID in the electronic environment.⁹

Mobile ID

Mobile-ID allows people to use a mobile phone as a form of secure digital ID. Like the ID-card, it can be used to access secure e-services and digitally sign documents, but has the added feature of not requiring a card reader. The system is based on a special Mobile-ID SIM card, which the customer must request from the mobile phone operator.¹⁰

Smart ID

Smart-ID works as an identification solution via a mobile application and thus does not require a SIM card in the mobile smart device.¹¹

With the ID-card each citizen also receives a personal @eesti.ee e-mail address. The government uses this email address to send important information. In order to use the @eesti.ee e-mail address, citizens must forward it to their personal email addresses.

The ID card contains a chip used to store digitised data about the user, such as the user's full name, gender, and national identification number. In addition, the ID system leverages public key cryptography as the mechanism for authentication. The ID cards use 2,048-bit open-source public-key/private-key encryption, holding two separate digital certificates: one for confirming the holder's identity, and the other to allow an individual to sign documents with a digital signature.

The ID card contains a chip used to store digitised data about the user, such as the user's full name, gender, and national identification number. In addition, the ID system leverages public key cryptography as the mechanism for authentication.

⁹ <https://e-estonia.com/solutions/e-identity/id-card>

¹⁰ <https://e-estonia.com/solutions/e-identity/mobile-id>

¹¹ <https://e-estonia.com/solutions/e-identity/smart-id>

The ID cards use 2,048-bit open-source public-key/private-key encryption, holding two separate digital certificates: one for confirming the holder's identity, and the other to allow an individual to sign documents with a digital signature.

The ID cards are used pervasively, in health care, electronic banking and shopping, to sign contracts and encrypt email, as tram tickets, and much more besides — even to vote. In all, the Estonian state offers 600 e-services to its citizens and 2,400 to businesses.¹²

In October 2017, the news broke that a security flaw existed in the cryptographic keys in about 750,000 Estonian national ID cards. This flaw potentially allowed the private keys of the users to be inferred from the public keys. The vulnerability, called the ROCA vulnerability, was discovered in one of the code libraries, “Infineon”, in the smart card system. It is important to note that for a public key cryptography system to work, while the public key is shared with everyone, the private key must be kept private. This flaw left the ID cards vulnerable to identity theft.

The Estonian prime minister, recognising the “imminent risk” of attack, announced that the certificates of affected ID cards would be disabled effective 4 November 2017. Updates to the certificates were also accordingly laid out. The updates were released in the form of a certificate update.¹³

The Estonian experience with a digital ID programme, while an example of one of the most highly sophisticated implementations, demonstrates the scale of the impact when vulnerabilities are discovered, even when a population is technologically savvy. Notably, despite that fact that Estonia has a small population, and boasts a highly developed infrastructure, it was necessary to take significant measures to mitigate the risk. In developing countries with vulnerable infrastructure and populations, the impact would likely have been much greater.

Additionally, while in this particular case the risks were considered “theoretical” and authorities were able to avoid irreparable damage, had the vulnerabilities metastasized, the impact could have been much worse and the effort to restore normalcy more drastic. Estonia’s response in this case was prompt. Most developing countries have not and would not be able to respond with such vigour and promptness due to multiple factors, including capacity gaps and lack of awareness within the public and implementing agencies. The Estonian example, a

¹² “*Estonia takes the plunge*“, The Economist, June 28, 2014, (Accessible at <https://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge>)

¹³ <https://www.id.ee/?lang=en&id=38239>

near-miss with catastrophe, is also an argument against the push for biometrics-based digital IDs. Estonia uses public key cryptography as the authenticating attribute, and this may provide a more secure, rights-respecting alternative to biometrics.

Tunisia

Envisaged as a project to improve the quality of administrative services and operations,¹⁴ Tunisia first saw a draft law¹⁵ introducing changes to the current national identity card in July 2016. While the current ID card contains a unique identifier number and barcode, the legislation proposed amending Law No. 27 of 1993 on the national identity card¹⁶ to further equip the card with an electronic chip that contains sensitive personal data.

At first, the project garnered favourable media attention, given the country's post-revolutionary focus on combating corruption and advancing administrative reforms. However, once the draft became public for all to see, leading civil society activists — both in Tunisia¹⁷ and globally¹⁸ — as well as the leadership from the national data protection authority, began to shed light on the privacy implications of the bill, which we explore below.

The Ministry of Interior presented to the Ministerial Council the draft law to amend current legislation on national identity cards. The Ministerial Council approved and submitted the draft to the Assembly of the Representatives of the People (ARP) on 27 July 2016. The draft was then assigned to the legislative Commission on Rights and Liberties for review and amendments.

This initial draft contained provisions representing a severe threat to the protection of Tunisians' personal data, privacy, and cybersecurity. It contained vague, ambiguous language, and lacked essential safeguards for privacy. For example, Article 2*bis* of the initial draft stated: “[The encrypted part of the chip will contain] the administrative data related to the digitisation and registration of the

¹⁴ “En Tunisie, le projet de modernisation de la carte d'identité nationale inquiète les ONG”, Jeune Afrique, 1 December 2017, <http://www.jeuneafrique.com/495963/societe/en-tunisie-le-projet-de-modernisation-de-la-carte-didentite-nationale-inquiete-les-ong/>.

¹⁵ Basic Draft Law amending and completing Law No. 1993-27 of 22 March 1993 on the National Identity Card, https://www.accessnow.org/cms/assets/uploads/2017/08/Tunisia_CIN_Draft_ENG.pdf [English translation], http://www.anc.tn/site/servlet/Fichier?code_obj=94673&code_exp=1&langue=1 [Original Arabic].

¹⁶ Loi n° 93-27 du 22 mars 1993 relative à la carte d'identité nationale: <http://www.legislation.tn/sites/default/files/journal-officiel/1993/1993F/Jo02493.pdf>.

¹⁷ Access Now, “Tunisia: Statement on Proposed ID Card,” <https://www.accessnow.org/tunisia-statement-proposed-national-id-card/>.

¹⁸ Experts Cast Doubt on Tunisia's Biometric Identification Bill, Global Voices, 30 November 2016, <https://advox.globalvoices.org/2016/11/30/experts-cast-doubt-on-tunisias-biometric-identification-bill/>.

card”. Nowhere in the draft were the terms “digitisation”, “registration”, and most importantly, “administrative data” defined. This left the door open for all sorts of personal information to be included in the chip.

The initial bill also raised serious concerns for data security. The draft consolidated access to Tunisians’ sensitive personal information such as biometric data (like fingerprints), address and date of birth, into a single database, creating a single point of failure in the case the data is hacked or stolen. The draft did not indicate what kind of data would be stored, who would have access to it, or what measures would be taken to ensure the data would be secure. Worse, the bill did not give Tunisians the ability to access the information about themselves that would be stored on the card — imposing a five-year prison sentence for anyone who tried — while leaving in provisions giving police, national security agencies, and administrative agents broad access to rich data profiles of millions of citizens.

Roughly a year later, on 7 July 2017, the Commission on Rights and Liberties completed its review. The bill was supposed to be debated at the plenary session on 18 or 19 July 2017.¹⁹ But because of other legislative commitments, the debate was postponed and the draft was sent back to the Commission on Rights and Liberties. The bill remained there until it was finally placed on the plenary’s agenda for 9 January 2018.

On 4 January 2018, Chawki Gaddes, head of the national authority on data protection (INPDP), spoke before the Commission on Rights and Liberties to discuss the risks the bill poses to data privacy, clarifying that it was not the biometric format per se that was problematic, but the alarming absence of protections and guarantees for the privacy and personal data of citizens.

A day later, the Minister of Interior, Lotfi Brahem, spoke before the same Commission to argue for passage of the bill. He claimed that nobody “could hack the personal data of any individual, and that the Ministry of Interior is a strongly protected entity”, adding that Tunisians must “trust that”.²⁰ Legislators were not convinced by the minister’s testimony, adopting several amendments to ensure the safety of all Tunisian personal data the day before the bill was scheduled to hit the plenary floor. The amendments the legislators adopted abolished the creation of a national database. In the course of the debate, many insisted that while having

¹⁹ The actual date of completion of review and publication of meeting minutes and report by the Commission on Rights and Liberties was 18 July 2017. See report (Arabic) here: http://www.arp.tn/site/servlet/Fichier?code_obj=99034&code_exp=1&langue=1.

²⁰ “Lotfi Brahem : Le système de ministère de l’Intérieur ne peut être piraté,” Kapitalis, 6 January 2018, <http://kapitalis.com/tunisie/2018/01/06/lotfi-brahem-le-systeme-du-ministere-de-linterieur-ne-peut-etre-pirate/>.

fingerprints in the card itself could be useful for verification purposes, storing them in a national database raises digital security concerns that provide anything but safety.

On 9 January 2018, the day the amended draft was scheduled to go to plenary, the Ministry of Interior withdrew the bill from the docket of the Assembly of the Representatives of the People (ARP). While this means the bill was defeated in the legislative context for now, fears remain that the government will bring the project back either through an executive decree to change “technical specifications” or through another bill presented to the ARP under a different political composition, following the next legislative elections.

It is important to note that the draft bill amending the identity card law in Tunisia was withdrawn once amendments protecting citizens’ fundamental right to privacy were adopted. The amendments removed the necessity of maintaining a database at all — for example, following the revisions to the bill, authorities could take fingerprints for the sole purpose of including this data on the chip, but the data was then mandated to be destroyed. This, in essence, ensured that the fingerprints would act solely as a tool of authentication. While global human rights organisations celebrated the victory, they are cognizant of the Ministry’s intention to go on with the process and remain vigilant to ensure that Tunisia meets its human rights obligations with whatever identity programme may be proposed.

India

India’s national programme for Unique ID (UID) , known now as “Aadhaar” (a Hindi word that loosely translates to “foundation”), was established in 2008. It is a unique 12-digit number, provided to each resident of India, which is linked to a person’s biometric and demographic data. With more than one billion claimed enrollments in India, it is considered the largest biometric-linked national ID system in the world.

This was not the first national identity-related project undertaken by India’s Union Government. The first major one was an explicitly national security-focused ID card effort launched soon after the conclusion of the Kargil conflict, with the objective of having all Indian residents enrolled in a National Population Register which would distinguish between citizens and non-citizens. In 2008, the new administration began work on a Unique ID effort broadly focused on creating a

master database that would track social welfare programmes in order to de-duplicate “ghost beneficiaries”.²¹

When established, authorities said the Aadhaar Unique ID would be voluntary and would help the Indian government achieve the twin objectives of (1) close gaps in welfare delivery systems through better targeting, and (2) increase the efficiency of welfare delivery systems by leveraging technology.

The Aadhaar ID programme is administered by a government-run (and now statutory) entity called Unique Identity Authority of India (UIDAI). Enrollment of residents into the scheme -- including the collection of biometrics -- has been done through agencies selected by the UIDAI, comprising of a wide spectrum of private vendors along with public sector agencies. The primary idea behind Aadhaar has been proper authentication of identity, through requests sent by requesting agencies to the central database of Aadhaar: the Central Identities Data Repository (CIDR). The requesting agencies ask for authentication by sending Aadhaar information along with the demographic and/or biometric information of the authenticatee. The CIDR has all the information of individuals registered under Aadhaar. The CIDR processes each request and provides a yes/no reply along with other information to the requesting agency. In the case of “know-your-customer” or KYC authentication under the Aadhaar programme, the CIDR returns “e-KYC data” (electronic know-your-customer), which includes the demographic information as well as the photograph of the authenticatee. Such KYC authentication can only be done using biometric information, or one-time passwords generated and transmitted to the registered mobile number of the authenticatee.

Over the years of its operation, the Aadhaar scheme has become more explicitly connected with the Government of India’s digital service delivery and tech-enabled civic engagement efforts. Aadhaar has been cast as a major pillar of the current Union Government’s Digital India programme for government services that are made available to citizens electronically. As a result, Aadhaar has been tied to multiple services, from banking and internet services to international travel and marriage registration. Aadhaar use by private tech firms with respect to their consumer-facing digital services has also been on the rise, and there have been reports of Facebook testing new logins to its platform that would require Aadhaar.

21

<https://scroll.in/article/825103/aadhaar-shows-indias-governance-is-susceptible-to-poorly-tested-ideas-pushed-by-powerful-people>

²² All these services are envisioned to use authenticating services as described above.

Use of Aadhaar has not gone without significant controversy and challenge in India. Aadhaar has faced a gamut of issues which can be divided in the following buckets: (1) implementation issues, (2) privacy issues, (3) security issues and (4) surveillance issues.

Implementation issues

According to its supporters, Aadhaar was envisaged primarily as a tool for better delivery of welfare provisions in India. However, multiple technological and infrastructural problems such as connectivity issues, hardware malfunctions, and duplication have hindered the effective application of Aadhaar for this purpose. Stories of old women unable to access services because their fingerprints do not work on the authentication machines are important to illustrate the gap between the Aadhaar concept and the reality. Prominent economists such as John Dreze have written extensively on the subject of exclusion of citizens from welfare delivery due to the implementation of Aadhaar.²³ Scholars and public interest groups have indicated that the requirement for Aadhaar enrollment and authentication for an ever-increasing number of welfare schemes and government entitlements has caused considerable harm and exclusion for India's poor, particularly around Aadhaar-triggered exclusion from the public distribution system (PDS) for foodgrains, causing starvation and restrictions on social security, particularly harming the elderly and disabled.²⁴

Questions have also arisen about the narrative that Aadhaar has helped provide identities to those who did not have them before, with data uncovered by Right to Information Act requests indicating that only 0.3% of the 840 million Indian residents who had obtained Aadhaar as of 2015 had taken the "Introducer" route available to those without existing proof of identity. The overwhelming majority appear to have obtained Aadhaar

²²

<https://economictimes.indiatimes.com/tech/internet/want-to-open-a-facebook-account-keep-your-aadhaar-card-by-your-side/articleshow/62267904.cms>

²³

<http://indianexpress.com/article/opinion/columns/aadhaar-biometric-authentication-abba-public-distribution-system-pds-jharkhand-4946834/>

²⁴ <https://thewire.in/government/aadhaar-right-to-food-pain-exclusion>

enrollment using their existing authenticated documents to establish identity and address.²⁵

Privacy issues

India's regulatory framework for privacy, or the lack thereof, has been one of the most contentious points in the discourse around Aadhaar. Many individuals and organisations active in the Indian digital rights community have repeatedly expressed concern that the Aadhaar programme is not consonant with principles of privacy, which the Indian people should be inherently provided.

The Supreme Court of India is currently hearing a series of challenges to the Aadhaar programme. A constitutional bench of the Supreme Court²⁶ is holding hearings to determine the legality of the programme. One of the key pillars of the challenges to the Aadhaar scheme is its abrogation of the fundamental right to privacy.

The Supreme Court of India, in its seminal judgement in the *Puttaswamy v. Union of India* case in 2017,²⁷ affirmed that each Indian has a fundamental right to privacy under the Constitution of India. However, the impact of this judgement on the fate of the challenges to Aadhaar is yet to be determined. The primary argument with regard to privacy is the semi-coercive nature with which the state is capturing biometric data and building a centralised database. While Aadhaar is considered a voluntary scheme, over time, the government has made Aadhaar necessary for carrying out basic functions in society, such as filing taxes or getting rations or even using a bank account and conducting a range of private sector activity, including the activation of telecom SIM cards. This has, in effect, made Aadhaar mandatory for the Indian public. It is being argued that requiring people to provide their biometric data to get services violates the fundamental right to privacy, and

²⁵

<https://www.hindustantimes.com/india/very-few-indians-didn-t-have-id-proof-before-aadhaar/story-0v4U95UH57i0O0snYE1EeN.html> (For background: "People can enroll for Aadhaar in two ways. They can submit authenticated documents to establish their identity and place of residence. These include an array of identity proofs people already have, such as voter cards, passports, ration cards, driver's licenses, and PAN cards. The second option is going through an "introducer" system in which an Aadhaar number holder authenticates the credentials of an applicant. This means that a person can get an Aadhaar card without possessing any other documents.")

²⁶ A constitution bench of the Supreme Court of India consists of five or more judges specifically appointed to only hear cases involving a substantial question of law as to the interpretation of the Constitution of India.

²⁷ http://supremecourtindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

does not comport with the necessity and proportionality standards that determine the exceptions to the right to privacy.

The Government of India, for its part, has taken steps to formulate a legal framework for data protection in India. This framework is supposed to address the questions related to Aadhaar, privacy, and more. In order to build this framework with expert input and stakeholder consultation, India's Ministry of Electronics and Information Technology created a committee under the chairmanship of former Supreme Court Justice Shri B N Srikrishna.²⁸ This committee has been tasked with producing a report and a draft bill on data protection, and is expected to publish its recommendations in the summer of 2018. The prior UPA government had previously established a committee of experts under the Planning Commission chaired by former Delhi High Court Chief Justice AP Shah, which published a 9-point focused report,²⁹ in addition a departmental effort working on an inter-ministerial draft legislative text for a proposed privacy bill across 2011-2015.³⁰

Security issues

The security of the data under the Aadhaar programme is yet another disconcerting issue. Repeated reports of data breaches and the exposure of personal information,³¹ and biometric replay attacks along with access to the database by unauthorised persons,³² signal not only the deficiency of protections provided by law, but also deficiencies in the technical architecture and safeguards for Aadhaar.

The use of biometrics as a authentication mechanism carries significant security risk. Given the unique and singular nature of biometric information, biometric leaks may be irreversible. Unlike a system that relies on a password,

²⁸ <http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited>

²⁹ http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

³⁰ See

<https://cis-india.org/internet-governance/high-level-summary-and-critique-to-the-leaked-right-to-privacy-bill-2011>, <https://iltb.net/comments-on-the-privacy-bill-2011-8b916ca96a81>.

³¹ <http://indianexpress.com/article/india/govt-admits-aadhaar-data-leak-critics-cite-civil-liberties-4639819/>;
<https://www.medianama.com/2017/04/223-aadhaar-leaks-database/>

³²

<http://www.financialexpress.com/india-news/aadhaar-data-hack-iit-kharagpur-graduate-arrested-earns-rs-40-lakh-a-year-at-ola/793999/>;
<https://www.bloombergquint.com/law-and-policy/2018/01/04/aadhaars-security-questioned-again-are-indians-at-risk-of-identity-theft>

in the Aadhaar system, once biometric information is compromised, you may be unable to restore a pristine identity.³³

While encryption can enhance security to a central database, experts such as Bruce Schneier consider that such systems are liable to breach through attacks on computers using the data.³⁴ Even if the encryption is not cracked, it is liable to be circumvented. News reports of data breaches by collection agencies, along with replay attacks to bypass authentication, further signal unaddressed vulnerabilities. Another reason for concern highlighted by Troy Hunt is the centralisation of data, an inherently insecure means for storing data.³⁵ A central database creates a single point of failure. While one may employ the best mechanisms of securing a database, it is the cybersecurity equivalent of putting all your eggs in one basket. Security researchers have also pointed out the flaws in the cybersecurity culture for the Unique ID Authority of India: it does not have a public bug disclosure programme,³⁶ in addition to issuing subordinate legislation to treat its cybersecurity policy framework as classified and deny Right to Information Act disclosure requests.³⁷

Surveillance issues

The authentication mechanism under Aadhaar system leads to the creation of authentication logs. Each time Aadhaar is used to authenticate one's identity, the log notes metadata of such authentication. Experts have noted that when done at scale and over a long period of time, such authentication logs can be a tool for pervasive profiling and surveillance.³⁸

In addition to the data being stored, the standards for such data being shared with law enforcement and other agencies is another cause for concern. The legislation provides a broad standard of “national security” which must be assessed while evaluating requests for data, and overall, uses a legal process

³³

https://www.buzzfeed.com/pranavdixit/one-id-to-rule-them-all-controversy-plagues-indias-aadhaar?utm_term=.nupprgWOk#.ga7mlQ0qz

³⁴ Ibid

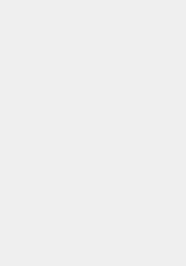
³⁵ Ibid

³⁶ <https://medium.com/karana/a-billion-users-but-no-bug-reporting-policy-20ce35122795>

³⁷

<https://scroll.in/article/830589/under-the-right-to-information-law-aadhaar-data-breaches-will-remain-a-state-secret>

³⁸ https://www.schneier.com/blog/archives/2014/03/metadata_survei.html



that is weaker than that in Indian law regarding the interception of telecommunications data.³⁹ It must also be noted that currently, only the executive branch of the government is involved in making and evaluating such requests, with a lack of judicial oversight of the process. It is illustrative to note that recently the government of Uttar Pradesh processed and accepted 10,000 telephone surveillance requests in two days.⁴⁰

III. TERMS FOR THE NATIONAL DIGITAL ID DEBATE: DEFINITIONS

- Authentication** Authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity.⁴¹ Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.⁴²
- Authenticator** An authenticator is any type of information that can be used to verify a person's identity. The classic paradigm for authentication systems identifies three factors as the cornerstones of authentication: (1) something you know (e.g., a password), (2) something you have (e.g., an ID badge or a cryptographic key), or (3) something you are (e.g., a fingerprint or other biometric data).⁴³
- Biometric data** Biometric data are characteristics that are unique personal attributes that can be used to verify the identity of a person who is physically present at the point of verification. These characteristics can be physical or behavioral. They include facial features, fingerprints, iris patterns, voiceprints, stride recognition, and many other characteristics.⁴⁴ In the context of the national identity programmes discussed in this paper, biometric data are often used as authenticators to verify the cardholder/user's identity. Biometrics may be imprinted onto the

³⁹ Under the Indian Telegraph Act (Section 5 and Rule 419A of the Telegraph Rules) and an analogous provision of the Information Technology Act (Section 69), interception of communications can only be authorised in ordinary circumstances by the senior civil servant heading the home department at either the Union Government or state government levels for certain specified grounds subject to meeting the preconditions of "public emergency or imminent threat to public order". In comparison, the Aadhaar Act allows for Aadhaar information to be handed over on the direction of a more junior level of civil servant (a joint secretary) on the grounds of "national security", a term not legally defined in India.

⁴⁰ <https://thewire.in/213729/adityanath-phone-tapping-uttar-pradesh/>

⁴¹ National Institute of Standards and Technology, Special Publication 800-63, "Digital Identity Guidelines," <https://pages.nist.gov/800-63-3/>, page iv.

⁴² *Id.* page vii.

⁴³ *Id.*, page 12.

⁴⁴ NIST Digital Identity Guidelines, page 13-4.

corresponding digital identity, or used in other ways -- such as the use of specific data points or formulas for successful stride recognition.

- Digital identity** While there is no standard accepted definition of digital identity, it generally refers to the online persona of an individual.⁴⁵ It is understood to contain the twin components of Identification and Authentication.⁴⁶ When these functions are accomplished digitally, such identity may be considered as a digital identity. There exist various models of digital identity, such as (1) the digital identity established is premised as being exclusive to a particular service,⁴⁷ or (2) the identity is common to multiple services, and serves as the nodal identity of the individual in the digital ecosystem.
- Identification** Identification is the process of establishing information about an individual using an attribute or set of attributes that uniquely describe a subject within a given context.⁴⁸ Today this often involves examining “breeder documents” such as passports and birth certificates, consulting alternative sources of data to corroborate the identity being claimed and potentially collecting biometric data from the individual.⁴⁹
- Personal data** Personal data in most contexts refers simply to information about an individual. The primary test for data or information to be considered as personal data is “identifiability”. Multiple jurisdictions have classified data as personal data if a person is identified or reasonably identifiable from such data.⁵⁰
- Sensitive personal data** Certain personal data are considered to be more sensitive and revealing than other personal data. Such data are referred to as sensitive personal data. Any unauthorised processing of such data results in an intrusion and interference with users’ rights and such data is considered a matter of higher intimacy and privacy interest. Multiple jurisdictions⁵¹ have listed such data including health

⁴⁵ NIST Digital Identity Guidelines

⁴⁶ Omidyar Network-Hyperion, “Digital Identity, Issue Analysis report, http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Omidyar-Network-Digital-Identity-Issue-Analysis-Executive-Summary-v1_2-1.pdf

⁴⁷ NIST Digital Identity Guidelines

⁴⁸ *Id.*, page 47.

⁴⁹ Omidyar Network-Hyperion, “Digital Identity, Issue Analysis report, http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Omidyar-Network-Digital-Identity-Issue-Analysis-Executive-Summary-v1_2-1.pdf, page 8-9.

⁵⁰ Article 4(1), EU GDPR; Section 2(1) of the Personal Data Protection Act 2012, Singapore; Section 2, The Personal Information Protection and Electronic Documents Act, Canada; Section 1, Protection of Personal Information Act, South Africa.

⁵¹ Article 9, EU GDPR; Section 6, Privacy Act, Australia; Section 26, The Protection of Personal Information Act, South Africa.

information, genetic information, biometric information and information about religious beliefs, ethnic or racial origin and information relating to sexual orientation. Non-sensitive data when combined over time can also constitute sensitive data, since the essence of such derived data would have the same characteristics as that of sensitive data.

Verification

Verification is the process of ensuring a claimant's possession and control of one or two authenticators within or about the identity card using an authentication protocol. To do this, a verifier [in national identity programmes, usually a state actor] may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.⁵²

IV. POLICY RECOMMENDATIONS

Our key recommendations flow from our experiences in various jurisdictions where national digital identity programmes are being considered, implemented, or are in the process of being implemented. As we note above, they fall under three pillars:

1. GOVERNANCE
2. DATA PROTECTION AND PRIVACY
3. CYBERSECURITY

Following these recommendations is a separate section with our proposed guidance regarding biometrics for ID systems, whether public or private.

GOVERNANCE

Those who push for national digital ID programmes, as discussed above, often cite ease of governance when they do not base their arguments on national security.⁵³ Establishing digital identity programmes is set within the context of making the delivery of services, including welfare benefits, more efficient and accurate, and reducing corruption by using technology to assist in clear identification and secure authentication. However, these programmes can themselves become impediments to governance and harm the provision of welfare services and the wider inclusion of citizens. In India, several scholars and analysts have noted that the deployment of such

⁵² Id., page 56.

⁵³ World Bank, World Development Report 2016, "Digital Dividends," page 147, <http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>.

programmes is leading to exclusion of citizens from social welfare and public services in several cases.⁵⁴

TO ADDRESS THESE ISSUES, WE RECOMMEND THAT LAWMAKERS:

1. Ensure a defined and restricted scope of use for the digital ID programme, provided for in the law.

Lawmakers must explicitly and clearly define the purpose of a digital identity programme. The government must clearly explain the scope of application and use to the public.

2. Make enrollment and use of the digital ID voluntary.

Enrollment in a digital identity programme must be optional. While a government may have a legitimate purpose for requesting a digital ID when individuals access government services (healthcare, education), it should not be a requirement for provision of these services. Not having a digital identity should not exclude a person from receiving the basic services that the government is mandated to provide. Public officials and policymakers should operate in a manner that reflects understanding the value of multiple forms of identity.

National digital identity programmes should work to enable user agency and choice. As such, governments should not make a single form of identity mandatory. This principle should apply to state actions whether explicit (e.g. -- the government making possession of a particular form of national digital ID mandatory by a specific law or edict) or coerced (requiring the national digital ID for services provided by other public agencies, or placing pressure on private

54

<https://www.dailyo.in/politics/pds-biometric-aadhaar-card-public-distribution-system-bpl-apl/story/1/20208.html>. See also Reetika Khera, Impact of Aadhaar on Welfare Programmes, *Economic and Political Weekly*, Vol. 52, Issue No. 50, 16 Dec, 2017, <http://www.epw.in/journal/2017/50/special-articles/impact-aadhaar-welfare-programmes.html>

companies and platforms to make use of such IDs mandatory).

3. Create independent and well-designed mechanisms for grievance and redress.

Individuals should have appropriate mechanisms to seek redress for grievances related to abuse or misuse of their personal data as well as for data breaches. To that end, public authorities should keep detailed logs when officers access retained data, and document and retain records detailing the purpose of such access.

4. Ensure inclusion at the enrollment stage, and no exclusion during implementation, due to technology or infrastructural capacity gaps.

Users should not experience any form of discrimination throughout the enrollment process. Technical prohibitions or infrastructural gaps should not prevent or prohibit users from accessing services during implementation. This requires building robust systems that keep only a minimal amount of information about people and can provide alternatives when there are problems with the system. Digital identity programmes administered or coordinated by public agencies must be created with the understanding that lack of internet access can exacerbate the exclusion of citizens, especially when their capacity to access government services, legal entitlements, or conduct transactions is linked to an identity ecosystem that requires constant connectivity for regular authentication.

PRIVACY AND DATA PROTECTION

National digital ID programmes are data heavy, both during enrollment and when transactions are regularly authenticated. This raises significant concerns for privacy and data protection.

Given that these programmes are handled by governments, there is an inherent public trust in and authority associated with the collection of these data. This can lead to the pervasive use of IDs and put at risk the

information that individuals provide under such programmes. Further, the sheer scale of these programmes requires well designed safeguards.

TO PROTECT PERSONAL DATA AND PRIVACY, WE RECOMMEND:

1. Limit the purpose for which these data are collected and used. Put in place proper measures to prevent user profiling based on the data volunteered.

In accordance with the international human rights principle of necessity,⁵⁵ governments should limit the data obtained from individuals to that which is strictly and demonstrably necessary to achieve a legitimate aim. That aim shall be clearly defined and publicised. Furthermore, lawmakers should put in place both security and legal measures to prevent user profiling.

2. Grant individuals rights related to their own data, such as accuracy, recitication, and opt-out.

For a digital identity to be empowering, frameworks must be built in a manner that is user-centric and enshrines transparency. People must be able to have access to the data collected through or associated with their digital identity, and the legal right and easy ability to correct anything in it that is in error. All participants in a digital identity programme must have the following rights at minimum:

- *Informed consent along with sound basis for processing:* Users should have informed consent to the collection of their proper data to be used within the digital identity programme. They should have the right to withdraw that consent at any time.
- *Accuracy:* Personal data shall be accurate and, where necessary, kept up to date. Users shall have the right to access, rectify, and erase their personal information. Users shall also have a right to be informed about the use of their personal data for defined purposes and be able to object to any

⁵⁵ *Id.*, Principle 3, <https://necessaryandproportionate.org/principles#principle3>.

processing of data that is not strictly necessary.

- *Retention limitation:* Personal data processed for any purpose shall not be kept for longer than is necessary for the purpose at hand.
- *Integrity and confidentiality:* Personal data shall be processed in a manner that ensures state-of-the-art security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Institute robust data protection frameworks to which digital ID programmes are subject.

National digital identity programmes must be subject to data protection frameworks, in addition to any specialised regulations that might apply to such programmes if they provide for supplementary stronger protections for users. Furthermore, governments must ensure that the programmes are answerable to an independent privacy commissioner or data protection authority.

State actors must be required to oversee and enforce strong protections for user data amongst private sector players who may be involved in the operation of national digital identity programmes or who provide services requiring authentication against such digital identities. State actors must take action in the framing and enforcement of regulations to ensure that third parties do not construct parallel centralised databases built around a person's national digital identity indicator.

4. Minimise the amount of and type of data governments and associated service providers collect.

National digital identity programmes must seek to limit the amount of personal information collected to what is strictly necessary in relation to the relevant purpose. This includes data collection by government agencies directly as well as by service providers or third parties allowed to develop or use such national digital ID ecosystems.

5. Restrict lawful interception and monitoring of digital ID use and implement measures for accountability.

Access of data maintained by any national digital identity programme by law enforcement or other state actors must be governed by relevant international legal standards, particularly the “Necessary and Proportionate” principles,⁵⁶ in the absence of stronger domestic safeguards set out by law. Biometric data as well as other key types of sensitive data, such as information for authentication or identification requests to the system, should be recognised as “protected information”. Relevant legal frameworks or regulations should institute access accountability measures, by, for instance, mandating that the issuer of the national digital identity must maintain an access log that is associated with the identity for the user to consult at any time. The access log should contain the following information: who accessed the data, when, where, and for what purpose.

CYBERSECURITY

An effective policy framework for a digital ID programme must be supported by an equally strong technology and cybersecurity framework. The collection of large amounts of personal information pertaining to identities -- including biometrics -- often form “honeypots” for criminals and other actors for malicious hacking and cyber intrusion. Additional challenges related to the secure communication of data during authentication must be met through proper encryption.

⁵⁶ Necessary and Proportionate Principles, <https://necessaryandproportionate.org/principles>.

WE RECOMMEND THAT LAWMAKERS:

1. Institute capable foundational technology infrastructure.

Effective establishment of nationwide digital identity frameworks requires robust technology infrastructure. This infrastructure is critical due to the following factors:

- Such programmes are heavily reliant on communications technology for all parts of their functions.
- Digital ID programmes form the basis of many welfare activities in various jurisdictions. Infrastructural lapses lead to severe on-ground adversities in the lives of the beneficiaries.
- Highly critical personal information is carried by the such identity frameworks. It is imperative that proper protection is provided to such information.

In this context, strong foundational technology infrastructure is critical. The technology infrastructure must be tested for robustness through various stress and penetration testing tools.

2. Ensure that data collection and storage are not centralised.

Centralised data collection and storage for national digital identity programmes -- particularly those involving biometrics -- poses grave dangers and should not be promoted. We recommend the following:

- **Decentralised storage architecture:** The architecture of such systems is crucial, and models based on federated identity providers, brokered digital identity providers, brokered credential service providers, or personal identity providers

give stronger protections for the rights of users.⁵⁷

- **Multiple IDs:** Multiple forms of ID are an effective alternative, as they create options and utility. The benefits of non-centralised systems in the space of digital identity must be recognised and furthered.

3. Separate the functions of identification and authentication and avoid creating transaction logs for authentication.

In certain models of national digital identity, the central agency acts as the nodal agency for identification as well as authentication.

The clubbing of the two functions creates a bottleneck for roll out and increases cybersecurity risks. The weakest link in the identity system could be leveraged to expose both the identity as well as the authentication layer. This can be avoided by separating the identification and authentication functions, as done under UK Verify (where the authenticator and the identifier are separate agencies) or a mechanism such as SecureKey concierge⁵⁸ in Canada (where concierge service only works as a mechanism of connecting the service provider and identification agency, while exchanging no personal data between the two agencies).

Most authentication agencies create a transaction log of the authentication requests sent with respect each user. Such logs, while not always capturing data per se, capture metadata in relation to the transaction where the authentication request originated. Using brokered models, as described above, the need for creation of such authentication logs can be

⁵⁷ Omidyar Network-Hyperion, “Digital Identity, Issue Analysis report, http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Omidyar-Network-Digital-Identity-Issue-Analysis-Executive-Summary-v1_2-1.pdf, Definitions available at page 12 to 15.

⁵⁸ <https://securekeyconcierge.com/about/>

minimised. In the least, such transaction logs can be separated from nodes where identity information is stored. These transaction logs are separate from access logs, which are controlled by the user.

4. Institute “privacy by design” principles in the programme.

Any national digital identity programme must consider privacy in its initial design. Prevention is much better than cure, especially when it comes to system architectures. It is thus essential that privacy is foundationally incorporated — in cooperation with data protection authorities, non-governmental legal experts, and civil society — in the administrative, legislative, and technical design of such programmes from the outset as well as throughout the subsequent lifecycle and deployment of the initiative.

5. Ensure that national ID programmes are based on models for secure communications, including providing end-to-end encrypted traffic as far as possible.

As discussed above, highly critical personal information is carried through programme networks. Thus, providing proper protection to the communication activities such as requests and responses for authentication is essential for ensuring security. End-to-end encrypted communications throughout any digital identity system is of crucial importance to ensuring digital security and must be established as far as possible.

6. Provide transparency in terms of disclosure of cybersecurity policies.

Steps must be taken to ensure that the cybersecurity policies and principles developed to safeguard the digital identity infrastructure are disclosed to the public. Given the public importance and scale of such projects, these disclosures must be made as a matter of a right to citizens.

Additionally, such practices would encourage review of the policies by experts and other stakeholders. This would inform the

government, open up issues for consultations, and lead to the development of more robust cybersecurity policies and a more secure ecosystem as a whole.

7. Provide a legal and policy framework that incentivises reporting and disclosure of vulnerabilities.

Any digital identity programme's efforts on security must encourage the participation of security researchers, and focus on ensuring a proper framework to support engagement with that community. In such a framework, the relevant authority engages with security researchers and encourages the disclosure of vulnerabilities. Government authorities should not directly or indirectly seek to intimidate or criminalise the efforts of independent security researchers seeking to engage with the potential vulnerability or exploits that may be uncovered in digital identity programmes.

8. Take steps to notify affected parties in case of breach of data.

Even with the most robust systems in place, data breaches may occur. In this context, measures to notify users of such problems must be put in place. Given that ID systems deal with personal and sensitive data, while robust data breach prevention mechanisms must be put in place, complementary systems must also be implemented to notify affected users when data breaches do occur. Notification of users about the fact of a data breach and the potential impact on their data must be enshrined as a legal requirement. It is important that grounds of national security are not used to keep such information confidential.

V. USE OF BIOMETRIC DATA IN ID SYSTEMS: SPECIAL CONSIDERATIONS

Biometric identifiers have become increasingly popular in the public and private sectors as a means of identifying individuals and providing an alternate pathway for user authentication.

Generally, biometric identifiers include fingerprints, DNA, signatures, and retina and iris patterns. However, identifiers such as vein patterns, facial geometry, or even voice patterns, may be used. Biometric data is vulnerable to hacking just like other authentication methods, but unlike a password, biometric indicators cannot simply be reset as needed. This poses a higher security risk, since it becomes increasingly difficult to “make good” leaks or hacks of biometric data, and thus restore sanctity to biometric based systems.

The collection and use of biometric data poses significant risks for individuals. Given the potential for exploitation of these data, we discourage the use of biometrics in digital ID programmes. In its policy handbook for 2017, the Cato Institute advocates against use of biometric identification in national digital ID systems.⁵⁹ The aggregation and use of biometric data should be sharply limited, even if such aggregation and use is aimed at increasing convenience or justified as a way to enhance security.

RECOMMENDATIONS FOR THE USE OF BIOMETRICS IN DIGITAL ID INITIATIVES, WHETHER IN THE PRIVATE AND PUBLIC SECTOR:

**1. Avoid creation of centralised
databases of individuals’
biometric data**

Given the sensitivity of biometric information, and the fact that “restorability” is limited when information is compromised, we advise ensuring that such data are stored in a decentralised manner. A centralised database is more vulnerable, since it creates a single point of failure.

**2. Ensure that providing
biometric identifiers is
voluntary and opt-in, not a
default (security) measure.**

Individuals must not be compelled to provide identifiers. They must voluntarily opt in, and sharing identifiers cannot be a precondition for provision of services.

⁵⁹ Cato Handbook For Policymakers, 8th Edition (2017)
<https://www.cato.org/cato-handbook-policymakers/cato-handbook-policy-makers-8th-edition-2017/national-id-systems>

3. Minimise data collection and transfers.

Those creating digital ID initiative must minimise the collection and transfer of data associated with biometric identifiers. This can reduce risks and harm if the data are compromised. We recommend in general that developers employ on-device authentication when biometric identifiers are used as “passwords”, rather than using centralised cloud storage/authentication.

4. Develop legal procedures and evidentiary standards for biometrics with care to protect human rights and due process.

We must ensure care and due process when processing biometric data for evidentiary purposes. We recommend:

- When biometrics are used in criminal identification, the physical evidence should be retained and used as the primary source of identification. Law enforcement use of biometric data from consumer devices should be minimised.
- Biometric information collected by private parties must be recognised as “protected information”, subject to the legal standards required for such data under the “Necessary and Proportionate” principles.

VI. CONCLUSION

National programmes that create digital identities must, at their very conceptualisation, seek to protect the human rights of the individuals they serve. Poorly designed programmes, especially those that link to biometric data with centralised authentication and data storage, stand to violate these rights. Such centralised systems, which often operate with a heedless collect-it-all or link-it-all approach, introduce unnecessary risks with scant evidence of societal benefits. These programmes risk harming the interests of the same people that public officials and policymakers claim to want to help. Any digital ID programme that harms human rights is not acceptable, full stop.

Digital identity programmes must include in design and implementation sufficient safeguards and mechanisms to respect and protect the digital rights of the users. Failure to contemplate or build in these safeguards should force the shut down of deployment of these programmes, with meaningful restructure to better protect the human rights of users. In our recommendations, we urge decision makers to take action in the areas of governance, privacy and data protection, and cybersecurity.

Our approach stems from our experiences engaging in the development and implementation of national digital identity programmes around the world. The Indian example discussed in this paper illustrates the full spectrum of issues related to digital identity programmes that must be addressed to achieve desired objectives and protect human rights. The Tunisian example illustrates how civil society can take action to prevent harms from creating these programmes without fully considering the implications, either for human rights or security. The Estonian experience shows that even with the most sophisticated implementation, a national digital ID programme has significant risks, and using public key cryptography for authentication may be safer than using biometrics. The development of technologies such as blockchain demonstrates that there are alternatives to the current push for centralised, biometrics-linked national digital identity systems, even as questions remain about the best path forward.

We hope that readers of this working paper step forward with input and feedback. Technologists and leaders involved in government programmes for identity need to show both high level leadership and publicly demonstrate their responsibility to protect our fundamental right to privacy. It is best to acknowledge concerns early on, engage with stakeholders, and seek to meaningfully frame and implement a path forward that explicitly undertakes the protection of privacy as a legal and administrative priority.

For more information:

Naman M. Aggarwal (naman@accessnow.org)

Wafa Ben-Hassine (wafa@accessnow.org)

Raman Jit Singh Chima (raman@accessnow.org)

