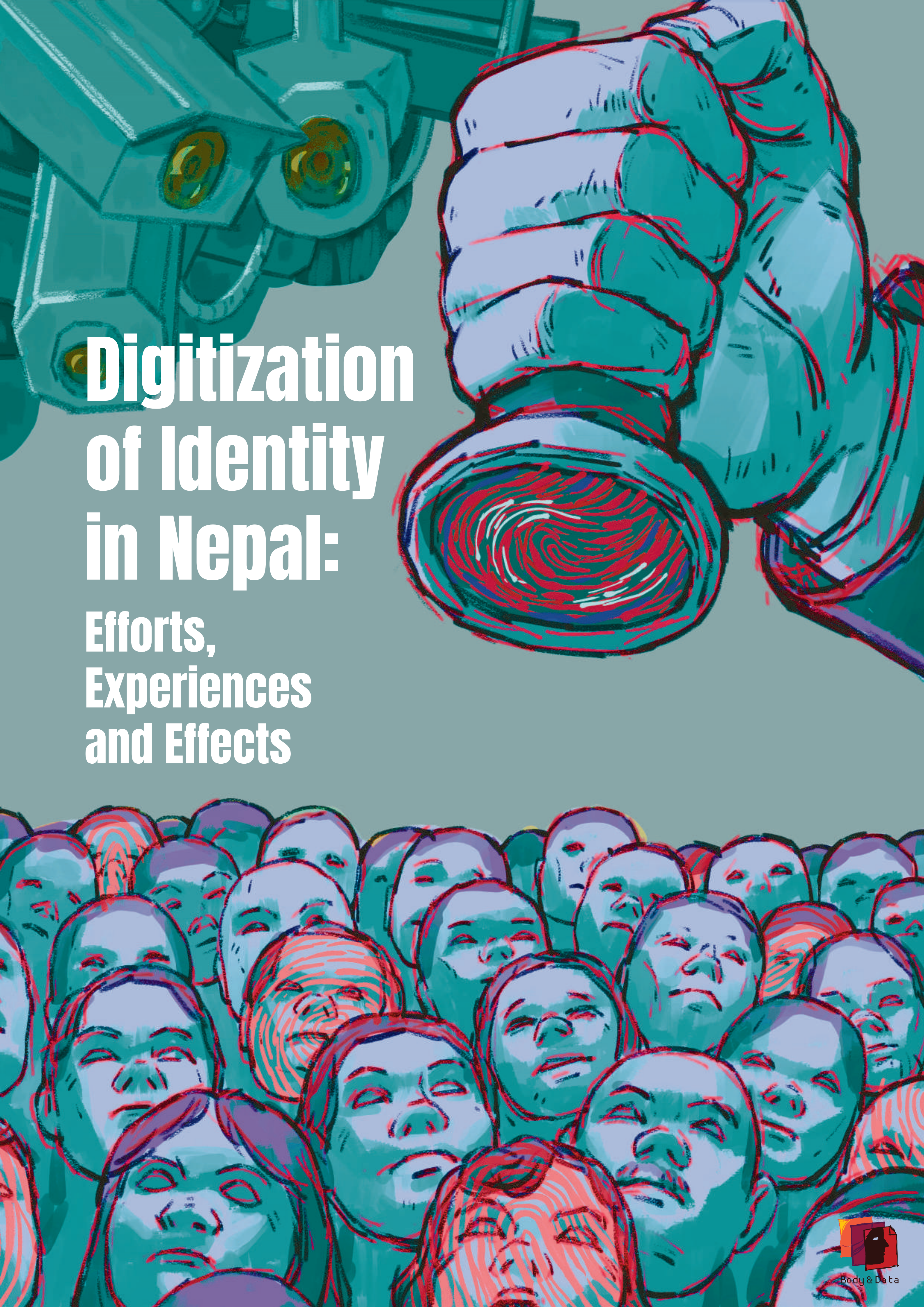


# Digitization of Identity in Nepal:

## Efforts, Experiences and Effects

Body & Data

**Digitization of Identity in Nepal: Efforts, Experiences and Effects**

This report is based on the study conducted by Body & Data in the districts of Panchthar (Phidim Municipality and Yangwarak Rural Municipality), Jhapa (Mechinagar Municipality, Kachankabal Rural Municipality, and Baradashi Rural Municipality), and Kathmandu in Nepal. The study would not have been possible without the contribution of time and knowledge from all the interviewees including the end-users, government officials at the local and central level, government-contracted data collectors, private sector representatives, and multilateral representatives.

**About Body & Data**
Established in 2017, Body & Data works to enhance understanding and access to information on digital rights among women, queer people and marginalized groups where they are able to exercise their rights in a safe and just digital space. We work towards the vision of accessible, safe and just digital spaces for all, through cross movement building, facilitation for access to information, knowledge building and dissemination on digital rights in the context of Nepal.

**Research Team**
Shubha Kayastha
Sapana Sanjeevani

**Research design and training**
Erica Diya Basu, Ph.D

**Interlocutors/local coordinators**
Surya Adhikari, Panchthar District, Phidim Municipality
Muna Bhattarai, Panchthar District, Phidim Municipality
Rajendra Kafle, Panchthar District, Yangwarak Rural Municipality
Radha Pradhan, Jhapa District, Mechinagar Municipality
Thanda Rajbansi, Jhapa District, Kachankabal Rural Municipality
Radhika Rajbansi, Jhapa District, Baradashi Rural Municipality

**Editing**
S. Rai

**Cover illustration and layout**
Supriya Manandhar

**Financial support**
Foundation for a Just Society (FJS)

# Contents

# Acronyms

| | |
|---|---|
| CDO | Chief District Officer |
| CSO | Civil Society Organizations |
| DDC | District Development Committee |
| DoNIDCR | Department of National Identity and Civil Registration |
| GDPR | General Data Protection Regulation |
| ID | Identity Document |
| NID Card | National Identity Card |
| NTA | National Telecommunications Authority |
| PIN | Personal Identification Number |
| PWD | People with Disabilities |
| UIDAI | Unique Identification Authority of India |
| USAID | United States Agency for International Development |
| WB | World Bank |
| WPF | World Privacy Forum |

# Terminologies used

The following terms have been used in this study based on the meanings below. We have used multiple sources including global legislations such as the General Data Protection Regulation (GDPR), definitions used by consumer and cybersecurity industry leaders, academic researchers, and civil society organizations (CSO) for this listing.

**Biometric Data** refers to personal data of the physical, physiological, or behavioral characteristics of an individual that has undergone some technological processing, which can confirm the unique identity of an individual. These can include but are not limited to, Voice Recognition, Fingerprint Scanning, Facial Recognition, Iris Recognition, Heart-Rate Sensors, etc. Biometric data digitally captures unique biological data for identity verification and authentication, but its use without adequate legal safeguards leads to extra-judicial surveillance by the state and private companies and raises critical data privacy concerns for individuals whose very bodies become a measurement of their personal lives.

**Demographic Data** refers to socioeconomic information/variables such as name, age, gender, address, marital status, religion, race/ ethnicity, level of education, employment, income level, etc. These can be expressed statistically to provide quantifiable representations among said populations.

**Personal Data** refers to any information relating to an individual such as a name, an identification number, location data, an online identifier, physical, physiological, genetic, mental, economic, cultural, or social identifiers, by which an individual can be directly or indirectly identified.

**Sensitive Data** fall under the special categories of a specific sub-set of 'special categories' such as racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; and biometric data (especially those processed to uniquely identify someone) that must be treated with extra security.

**Digital Literacy** builds on general literacy and reading skills to provide people with an understanding of how digital technology functions and how to use it effectively. This includes critical thinking and assessment of information, familiarity with various devices, the ability to navigate the Internet, and an understanding of issues associated with digital technology like data privacy, data breach, cybersecurity, informed consent, etc. (ScienceDirect)

**Digital Privacy** is a concept that individuals should have the freedom to determine how their digital information is collected and used. And they should have, at the bare minimum, the same protections by law as offline privacy.

**Information Security** refers to the processes and tools designed and deployed to protect sensitive information, in this case, online information, from modification, disruption, destruction, and inspection. They protect the confidentiality, availability, and integrity of online data. (Kaspersky & CISCO)

**Cybersecurity** is the application of technologies, processes, and controls to protect and reduce the risk of systems, networks, programs, devices, and data from cyber-attacks, and to guard against the unauthorized exploitation of such systems, networks, and technologies. (IT Governance UK & CISCO)

**Data Breach** is a cybersecurity incident wherein information is stolen or taken from a system without the knowledge or authorization of the system's owner. It exposes confidential, sensitive, or protected information to an unauthorized person/organization. The files in a data breach can be viewed/shared/altered without permission. Anyone can be at risk of a data breach — from individuals to high-level enterprises and governments. More importantly, anyone can put others at risk if they are not protected. (Multiple sources)

**Digitization**: The conversion of analog information, records, and objects into digital form.

**Digitalization**: The process of using such digitized information to change public and private policies in the belief that they are more efficient than their manual counterparts.

**Aadhaar Card/Aadhaar Number** is a 12-digit random number issued by the Unique Identification Authority of India (UIDAI) to residents of India after satisfying the verification process laid down by the UIDAI. Any individual, irrespective of age and gender, who is a resident of India, may voluntarily enroll to obtain an Aadhaar number. The Aadhaar number is a proof of identity and it does not confer any right of citizenship or domicile to the Aadhaar holder. (UIDAI website)

**Social Exclusion** is a complex and multi-dimensional process that involves the lack of or denial of resources, rights, goods, and services, and the inability to participate in the relationships and activities available to the majority of people in a society, whether in economic, social, cultural or political arenas. It affects both the quality of life of individuals and the equity and cohesion of society as a whole. (PSE UK)

**Profiling** means any form of automated processing of personal data of individuals to evaluate certain personal aspects relating to them, in particular, to analyze or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability scores, behavior patterns, and location movements. (GDPR)

**Machine Readable Passport** includes data on a passport that can be read by a computer. Specifically, the data is on the identity page of the passport and features the personal information of the passport holder. The machine-readable data usually consists of two lines of text, which are a mix of letters, numbers, and symbols. The data includes details such as the name, nationality, and passport number of the individual. When the text is scanned by a computer, the system uses character recognition to distinguish the personal details of the traveler.

**E-Passport**, **Electronic Passport**, or **Biometric Passport** is an international travel document with identity details such as passport number, name, surname, nationality, and date of birth, as well as an electronic microprocessor chip containing biometric data such as fingerprints, photos, and signatures. Biometric passports are scanned through special devices. (Multiple sources)

# Executive Summary

Biometric digital identity (ID) systems are being promoted by national governments, multilateral development agencies, and the private sector as the universal solution for legal identification, inclusive development, and accelerated economic growth to about 1 billion people without foundational IDs in Sub-Saharan Africa and Asia.

This pilot study examines the above premise against Nepal's National Identity Card (NID) apropos primarily the end-users' efforts to register, their experiences, and the effects of the program on their lived realities. The findings add weight to other global studies of national digital ID programs which reveal disturbing gaps between the promise and reality of implementing these systems.

When promoting the magic wand of digital IDs, governments and multilateral organizations often over-amplify tech solutions by conflating the goals of legal identification with inclusive growth and development, and underestimate the harms borne by the most vulnerable in our communities.

The use of biometric IDs, beyond simple identity verification and authentication, has the potential to become a near-continuous measurement of people's everyday lives through the collection, processing, and sharing of their unique bodily data. International digital rights organizations have reported that they exacerbate existing social inequities of marginalized groups like women (especially in patriarchal societies), people with disabilities, migrants, and transgender communities, leading to their further exclusion.

Biometric ID systems also depend on centralized databases storing and processing massive amounts of sensitive personal data without adequate attention paid to national cybersecurity capacities to ensure the confidentiality and integrity of data. The spate of massive national database breaches globally should give governments reason enough to rethink the necessity of interlinked centralized databases that have brought critical functions of impacted nations to a halt.

Moreover, digital national ID programs have often been designed and implemented without any consultations with civil society — the largest stakeholder group that these programs are purported to benefit and contrary to the participatory models of successful public development programs. Nepal's National Identity (NID) card program and the e-passport are similar cases – the latest in a series of physical and digital identity documents that Nepali citizens have been asked to register for, but from whom no consultation has been sought.

Our initial desk research on digital ID programs globally also revealed that these ID systems have oversized existential impacts on people's everyday lives. Their digital rights are often sacrificed against undue surveillance and privacy invasions of presumed technocratic, bureaucratic, and market efficiencies. Additionally, pre-existing marginalized communities are further excluded from political, social, and economic benefits when they are unable to register for these IDs.

More recently, multilateral agencies have begun to acknowledge the above-mentioned challenges of digital ID systems in the Global South and are looking for ways to encourage greater cross-sectoral sharing of knowledge, particularly between national governments and civil society organizations (CSOs).

At the time of writing this report, at a World Bank ID For Development (WB-ID4D) webinar, a leading digital rights advocate from Privacy International suggested that the

World Bank can and must leverage its position to make civil society consultations a funding requirement.

This could ensure that World Bank-funded countries conduct multistakeholder consultations before they design and implement these national digital ID programs. It could also help to assess if the countries have the requisite technological infrastructure, human resource capacities, and digital literacy levels to implement these projects within an inclusive, fair, and just framework.

As Nepali citizens, these issues concerned us when the government launched Nepal's national ID program following the heightened global trend of maximizing data collection on citizens through various public policies, eschewing multistakeholder consultations, increasing multipurpose usage with public and private organizations, as well as relying on a centralized database. As an organization, since 2017, Body & Data has been researching the digital space against the overarching mission and vision of digital rights for individuals with particular emphasis on marginalized and vulnerable communities. Studying Nepal's National ID Card, especially from an end-user perspective, fell well within the ambit of our objectives.

Since this was an exploratory pilot, we adopted a qualitative research methodology and used semi-structured interviews to collect rich, contextual, primary data which we used to analyze thematically vis-a-vis the secondary data of existing research, policy documents, and media reporting. Our commitment to multistakeholder consultations led us to also seek the perspectives of government officials, government-contracted data collectors, the private sector, and multilateral agencies – particularly those involved in the pilot phases of the program.

[Detailed Research Methodology & Methods included in Appendix A]

# Introduction

## *Digital ID programs*

In countries around the world, digital identity projects have become the preferred "one size fits all" solution offered by multilateral development agencies, national governments, and technology management consultancy companies. Digital ID projects promise to meet a diverse range of challenges from meeting the United Nations goal of providing legal ID for the billions of undocumented people to the efficient delivery of government services, cost-effective private sector identity verifications, and the elusive promise to the end-user of easier access to public and private sector services.

However, in Global South countries these all-encompassing digital ID projects have fallen short of their implicit benefits. They have more often than not been implemented without the participatory consultation of civil society. This exacerbates existing social inequities of marginalized and vulnerable populations based on gender, sexuality, ethnicity, ability, religion, class, and caste, resulting in exclusion rather than inclusion.

These national digital ID projects have ignored the principles of proportionality by over-collecting sensitive biometric and demographic data of citizens. The data is then indiscriminately shared across the public and private sectors resulting in extra-judicial state surveillance and consumer targeting within weak rule of law environments to meet other political and commercial imperatives beyond legal identification and delivery of services.

Furthermore, these countries also suffer from unstable internet infrastructure, poor digital connectivity, and very low levels of digital literacy among the majority of end-users. End-users are not aware that less than adequate attention is paid by policymakers to observe universally accepted standards of informed consent that safeguard people's digital rights.

As Nepal is a late entrant to the digital ID bandwagon, we first wanted to place Nepal's NID card within the Global North-South continuum. We then wanted to examine other Global South experiences and civil society interventions to identify points of convergence and divergence in analyzing the findings of this study.

## *Nepal's NID card and the global context*

Although the Government of Nepal introduced the NID program in 2010 it did not implement it then because there was no legislation to back the policy. It was only after Nepal's Constitution was promulgated in 2015 that the Department of Civil Registration started to develop the information system for data storage.

Since then, the government has passed the following three legislative documents for the NID Card and Civil Registration:

- The NID Card and Civil Registration Act, 2076
- The NID Card and Civil Registration Regulation, 2077
- Procedure for Conduction of NID Card Program, 2077

A worrying fact is that while the NID Card and Civil Registration Act was passed on February 11, 2020, enrolment in the NID program in Panchthar district began two years prior in 2018. This early registration is tantamount to an unconstitutional collection of data.

The first two pieces of legislation describe the creation and administrative functions of the Department of NID & Civil Registration (DoNIDCR) to implement the NID and other civil registrations. It allows the DoNIDCR to record the demographic and biometric data of an individual for the national ID and other vital registration including updating and correcting erroneous data. It also allows the department to issue the NID number and NID card. It provides the legal basis for developing an Integrated National Identity Management Information System and links it with services provided by the state and other agencies that have legal permission from the Government of Nepal.

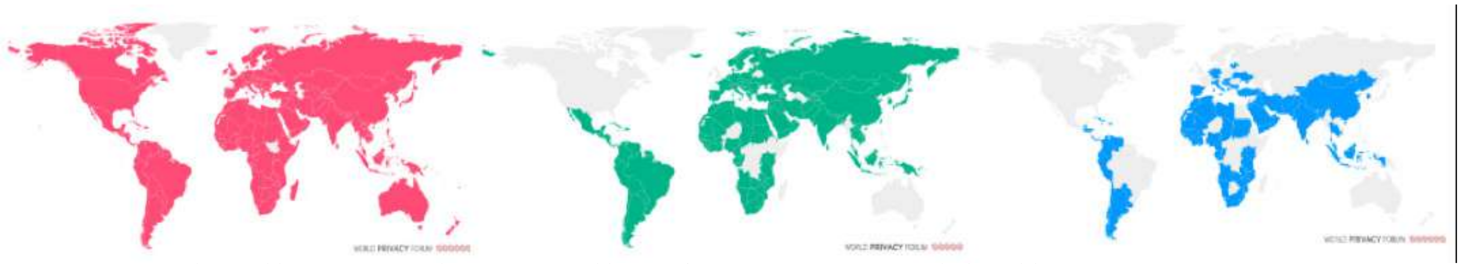
However, more important is the Procedure for Conduction of the NID Card which provides the constitutional and legal basis for the program. State Policies relating to national unity and national security in the Constitution under Article 51(a) – particularly section (3) – allows the state, "to maintain law and order by developing a national security system".

It allows the department to develop and establish a central integrated information system for the NID Card program and opens the way for the government to manage detailed demographic and biometric information of citizens and integrate such sensitive personal data with other service-providing agencies. These finer details about data sharing between government agencies and authorized organizations are not widely known by most citizens in Nepal. These details are not communicated to end-users during their enrolment and make the concept of 'informed consent' a de facto mockery.

The NID card, according to the Director-General of the DoNIDCR at a public meeting, will replace the old citizenship card. It is envisioned as a unique number assigned to every Nepali citizen to give them easier access to government services. It can also be used by authorized private sector service providers, such as banks and mobile phone companies, for identity verification and authentication purposes.

We used the World Privacy Forum's (WPF) interactive global map for NIDs and noticed some stark differences between the Global North and South countries.[1]

The three WPF maps below provide a graphic illustration of the global scenario for NIDs. Red represents nations with National IDs, green where national IDs are digitized, blue where biometrics are collected for National IDs.



*Map Credit: World Privacy Forum. https://www.worldprivacyforum.org/2021/10/national-ids-and-biometrics/*

[1] (National IDs Around the World — Interactive Map, n.d.)

Although almost all countries have some form of a national ID, the number drops dramatically when you examine how many countries have digitized their ID systems and falls even further when you examine which countries have adopted biometric elements to their digital NID cards. The countries with biometric-based NID cards are concentrated in the Global South countries of Asia, Africa, and South America. Nepal has followed this troubling trend of other Global South countries by implementing a biometric-based NID card.

This trend is troubling because most Global South countries have very large and dense populations with low basic digital infrastructure and digital literacy levels, few data protection laws, and poor judicial oversight of surveillance and cybersecurity standards.[2] The Global North countries with relatively smaller populations, well-developed digital infrastructures, higher levels of digital literacy, national, state, or sectoral data protection laws, and far greater judicial oversight of surveillance and cyber security standards have not adopted biometric digital NID cards. This must give us pause to examine why the Global South countries are in such a rush to adopt them without the requisite internet connectivity, judicial, and literacy infrastructures to support and justify such large-scale digital policies en masse.

Biometrics-based technology is becoming an increasingly popular technological tool[3] in South Asia, presented as an efficient and anti-corruption innovation and can be found in use-case scenarios such as digital IDs, facial recognition technology at airports and police stations, and seemingly mundane purposes such as finger-print and/or facial recognition-based entry devices in apartment buildings. They are implemented citing efficiency and security, and embraced for their technological novelty and convenience, without realizing they bring with them a new form of bureaucracy and surveillance infrastructures that come with both pre-existing and new complications of targeting and discrimination.[4]

We must also ask why multilateral finance and international development agencies push for these IDs in Global South countries. The political economy behind these large-scale digital ID projects in the Global South must be examined. Which private sector companies are involved in and stand to financially benefit from the design and implementation of these digital ID projects? While examining the political economy of Nepal's NID project is not within the scope of this study, we intend to pursue this line of inquiry as a future research project with partners globally as we feel it could yield some interesting results.

## Global south digital ID programs: challenges and civil society action

Global human rights organizations, scholars, and grassroots practitioners have all raised concerns that these mandatory national digital biometric cards are often not more efficient than earlier systems; the lack of internet connectivity results in them being used as physical IDs that completely negate the justification of ID deduplication used to promote them. This gives rise to various forms of social exclusion and puts the personal information of digitally vulnerable population groups at risk.[5]

[2] (Cyber Security in the Global South, 2017)

[3] (Best, 2010)

[4] (Fluri et al., 2015)

[5] (Digital IDs Rooted in Justice: Lived Experiences and Civil Society Advocacy towards Better Systems, 2022); (Aggarwal, 2018); (Sinha & Kodali, 2017)

Concurrently, civil society organizations in Global South countries have scrutinized their rapid deployment, and raised pertinent questions apropos their country; they question if these countries have the requisite internet infrastructure resources, stable digital connectivity, and affordable data access plans to support such massive-scale digital policy programs.

Others have questioned whether the governments have data protection laws and judicial oversight to protect the digital privacy and information security of their citizens? Do these populations, particularly in vast semi-urban and rural areas, possess adequate digital literacy and awareness to ensure the safe and inclusive implementation of these cards with meaningful and informed consent? These CSOs have also examined the commitment of their governments to transparency, fairness, accountability, and a multi-stakeholder consultative process for designing and implementing programs since most of them, while embracing multistakeholder values at international internet governance forums, do not practice them in digital policymaking at home.[6]

For example, Kenya's NID card, popularly dubbed Huduma Namba, has faced civil society-led criticism that the card exacerbates the digital and structural inequities already faced by the poor and marginalized citizens, particularly in rural areas. This led to the deployment of the card being deferred till their courts sought further information about the negative externalities of the card on the end-users. Several civil-society critics and cybersecurity experts from India testified at these hearings to amplify the challenges faced by India's Aadhaar on which the Kenyan card was modeled. Kenya's High Court eventually decided that the program was illegally rolled out and should be halted till a privacy assessment study was conducted.[7]

Closer to home, in India, the civil society-led Puttaswamy case against its national, and the world's largest digital identity card 'Aadhaar', led to its Supreme Court adjudicating the fundamental right to privacy for Indians and putting in place limitations on the use of the card. It also demanded a collaborative consultative committee of government, private sector, and civil society representatives to ensure policy equity for all stakeholders.[8]

More recently, the January 2022 report from the Engine Room about Indonesia, Jamaica, Pakistan, and Uganda, revealed similar socio-political-economic inequities getting exacerbated by the deployment of such NID cards in their countries. In Indonesia, the lack of existing identity documents resulted in exclusion from the registration process itself and subsequent lack of access to government services that were linked to having the NID card. In Jamaica, civil society action led to the Jamaican Supreme Court citing India's dissenting voices and did not implement its national digital ID card on the grounds of a breach of privacy of Jamaican citizens[9].

Pakistan's civil society actors voiced concerns about access and safety for their citizens based on how far-reaching its Computerized National Identity Card (CNIC) was for availing both public and private services. Gaps in the registration process have led to the exclusion of some population groups from getting a card resulting in existential challenges for them, especially during COVID-19 where the national vaccination program was linked to the CNIC. They also fear data leaks and breaches of citizens' very sensitive data from the centralized government-held database. Trust in government

[6] (Abraham & Pattanayak, 2018)"; (Dixon, 2017); (Khera, 2018); (Khera, 2019); (Sinha & Kodali, 2017)

[7] (Sur, 2021)

[8] (Justice K.S. Puttaswamy (Retd.) & Anr. Vs. Union of India & Ors., 2017)

[9] (Robinson v. Attorney General, 2019)

is also very low in these above-mentioned countries. In Uganda, one of the primary criticisms was the lack of a multistakeholder framework that excluded civil society involvement and input in the design and deployment of its national digital ID card, called Ndaga Muntu. They feel that most of the exclusion and challenges that vulnerable populations face in registering and interacting with the authorities could have been mitigated with consultations with civil society groups representing these groups in the design phase itself.[10]

The lop-sided narrative, from governments and multilateral development finance institutions, is that people are excluded from public and private services because they do not have a verifiable legal identity. The ground realities however reveal that the mere possession of a national digital ID does not solve all issues of exclusion. The central authentication system of NIDs themselves can be highly exclusionary as was seen in the Aadhaar card system in India where rural starvation deaths occurred due to card authentication failure issues.[11] Another example is that safe abortion is permitted in India under certain conditions since 1971; although there are other socio-economic and cultural barriers to access them. With Aadhaar in place, many public hospitals in India are asking women to link their Aadhaar cards to access safe abortion and other reproductive health services; many women are nervous about what this data could be used for. This is not only affecting women's rights to access basic health care but also the privacy of women seeking reproductive health services.[12] We hope that the Nepal government will peruse this report and include us and other civil society organizations as it expands the NID program and continues to develop its Digital Nepal vision.

In the context of geopolitical and geo-economic security, states can use biometrics to further identify and control.[13] Biometric data can be used for surveillance, to track and identify hidden populations who have successfully avoided other forms of official identification.[14] The centralized data system in the digital economy combined with advanced technological features like algorithms can put a person's privacy at threat at various levels that the individual is completely unaware of when accessing goods and services online.[15] Oftentimes, the practice of collecting sensitive personal data is invasive, and much more data is collected than required for some future use scenario that the individual is not informed about.[16] A study conducted among key populations[17] in Kenya raised a serious concern that data stored for one purpose is later used for another purpose not originally consented to. In the case of Kenya, the concern stems from data gathered for health purposes that could be used by the police to target criminalized key populations for arrest in the context of same-sex sexuality, sex work, and drug use, which are all criminalized in the country.[18]

In addition, the collection and sharing of inordinate amounts of personal and non-personal data to develop and deliver internet-enabled digital products and services

[10] (Digital IDs Rooted in Justice: Lived Experiences and Civil Society Advocacy towards Better Systems, 2022)
[11] (Khera, 2017)
[12] ("Country Case-Study: Sexual and Reproductive Rights in India," 2020)
[13] (Fluri et al., 2015)
[14] ("Everyone Said No" Biometrics, HIV and Human Rights A Kenya Case Study, 2018)
[15] (Khera, 2018)
[16] (Aggarwal, 2018)
[17] Key populations, identified by UNAIDS as female sex workers, men who have sex with men (MSM), and injecting drug users, have the highest risk of contracting and transmitting HIV. (Population council website https://www.popcouncil.org/research/key-populations-at-risk-for-hiv)
[18] ("Everyone Said No" Biometrics, HIV and Human Rights A Kenya Case Study, 2018)

by governments, such as digital NID cards and the private sector's exploitation of user-data to algorithmically target groups, has also led to a growing trust deficit between citizens and their governments and large corporations.[19] Simultaneously information security, digital privacy, and digital rights concerns have risen to the top of global policy agendas and spurred citizen-led digital rights advocacy efforts to balance the needs of national development and human rights with adequate legal safeguards and judicial oversight[20].

# About this study

## *This Study's Relevance and Significance*

It is within the broader context and public discourse on digital policies and their impacts on the digital rights of people that this initial pilot study has been undertaken. Our primary goal was to map Nepali end-user's understanding of, experiences with, and expectations from Nepal's NID program.

The study adds to the existing scope of work that Body & Data has been doing in the digital space since 2017 around exclusion/inclusion, marginalization of certain population groups, increasing and at times disproportionate government and corporate surveillance capacities without adequate judicial and security oversight to protect the rights of all citizens.

We believe the initial findings from the two districts, Jhapa and Panchthar, could inform the government as it continues to expand the program's rollout, taking into consideration end-user perspectives. This would create a more holistic and justice-based framework to envision Nepal's digital future. This collaborative ethos should guide Nepal's digital policymakers especially since we are a member country of the UN's Internet Governance Forum which fosters the spirit of multistakeholderism and looks to expand the growth of the Internet for development. An increasingly datafied society without critical reflection on how this impacts the "data subjects" themselves oftentimes reproduces older structures and biases of inequality and discrimination. The finding of this study will help us, the datafied citizens, to examine these negative fallouts and demand from the "data collectors" (governments, multilateral agencies, and corporations) greater accountability through informed resistance. We can then start to repurpose and redesign a more participatory, responsive, and just society that acknowledges and corrects the asymmetrical power relations of data collectors and data subjects which further enforces discrimination through datafication[21].

From a global perspective, this study could serve as a more relevant template for other countries with heterogenous but smaller populations. As mentioned earlier, Nepal's all-encompassing NID program has been omitted from global comparative studies and this study fills a gap in the existing literature about biometric-based global digital ID projects.

## *The Study's Research Methodology and Methods*

Since this was an exploratory pilot study to understand and examine a largely unexplored digital policy in Nepal, we decided to adopt a qualitative and descriptive methodology. We used semi-structured interviews as a research method to collect our primary data from end-users. We also included a few government officials, the private sector, and representatives from multilateral organizations to gain a multi-stakeholder perspective of the program processes, uses, and challenges. Given that the pandemic

[21] (Leurs & Shepherd, 2017)

limited the mobility of the research team, the interviews were conducted over zoom or telephone calls which also came with its limitations and challenges.

A detailed note on the research methodology and methods is provided in Appendix A.

## The Sample Population

The sample population was selected from the two districts of Panchthar and Jhapa. The reason behind this selection of districts was because Panchthar, an urban district, was the first district that rolled out the NID program while Jhapa, a predominantly rural district, was chosen next, as it shares an international border district with India with a fairly large migrant population. We understand that all interviewees are also end-users. However, for the purposes of this study, the latter three categories were interviewed as representatives of other stakeholder groups.

- End-users – 31 (13 men and 18 women)
- Nepali citizens from the earlier mentioned municipalities of Panchthar and Jhapa districts
- Government – 7 (officials and contracted data collection/computer operators)
- Those employed in government offices at the DoNIDCR, local district/ward level, and government-contracted data operators/collectors for the NID program
- Private Sector Representatives – 3
- Individuals employed at private sector organizations
- Multilateral Agencies – 2
- Nepali citizens who work at the World Bank and the Asian Development Bank; both multilateral agencies were associated with the initial stages of the NID program

## The Study's Challenges and Limitations

It was difficult to arrange interviews with government officials and multilateral organizations in Kathmandu and we had to reach out several times to arrange interviews. This can often mean more time has to be allocated to ensure their perspectives and often led to us feeling frustrated with our levels of reach in these sectors.

It was also difficult to reach the government officials at the local units who were busy managing the pandemic in their districts.

This research is limited to municipalities in two districts as it is a pilot study. We chose Panchthar district since it was the first district where the NID project was implemented. The second district we chose was Jhapa because the data collection for the NID card was ongoing during this research and we felt we might be able to get some more immediate experiences.

We had to limit our interviews to phone calls and contact a few of the stakeholders through email due to COVID-19 travel restrictions.

This section situated this research within the broader context of digital policymaking in Nepal and within digital rights which is Body & Data's sphere of work. The following section will situate the NID program within the larger context of Nepal's internet infrastructure which is foundational for its smooth implementation, for other NID-linked private and public sector policies, and the overarching Digital Nepal Framework. This policy background enables us to then move onto the chapter on key findings.

# Key Findings

This section maps and examines responses primarily from the perspective of end-users. We have also included limited findings from other stakeholders, the government, the private sector, and multilateral organizations. These comments are juxtaposed with experiences of end-users within a multi-stakeholder framework to identify areas/issues of divergence and convergence. This is essential for designing, implementing, and assessing such public policy programs. We have also analyzed the findings vis-a-vis reports about other national biometric ID systems to provide a comparative and comprehensive context within Nepal's NID program.

The data from a total of 43 interviews (a detailed break-up of these interviews is provided in the preceding chapter About This Study) revealed five overarching thematic categories presented below. Each finding is discussed in detail in the subsequent sub-section entitled Discussions and Analysis.

## *Analysis of findings*

### Lack of systematic and complete dissemination of information

The end-users, private sector, and even government-contracted data collectors were not fully informed about different aspects of the card. Government officials, on the other hand, were more thoroughly informed and claimed they had used multiple platforms from local making to radio spots as part of their communication strategy. This may indicate that the information about the biometrics ID card is not shared systematically, revealing an unjust governing structure. Our desk research also indicates that globally there seems to be a lack of a clear understanding of biometric digital ID systems among various groups of stakeholders. A more holistic dissemination of information among the public by the government using several regional languages, different mediums such as making, door-to-door awareness programs, announcements on TV, FM and social media and community-level public engagement programs would have been helpful to fill the existing gaps in information. Further, regular multi-stakeholder consultations at different stages before implementation would have helped the public to gain a better understanding of the NID program.

Often, strategies to provide incomplete information are purposely used so that those who control all the information, retain power. If governments are more transparent about digital NID cards, citizens might trust and put their faith in institutions who implement these systems. According to our research the current situation is that most people do not know what it is really for, those who question the NID are not feeling the answers provide anything more than what the citizenship card already does, and are just following orders out of fear of penalties.

### The NID program and its relevance

Overall, end-users were not well-informed about the NID program and responded with ambiguity when asked what they knew about the card. Most of their responses were similar to the statements below and also highlights a 'do as you're told' approach:

> *"I don't know about it (NID). When the chairperson (of the ward) told us to register all of us villagers went after him to register." End-User 10*

When asked about the uses and benefits of the NID card, there were no clear responses from the end-users. Unprompted, most of them responded to the physical aspects such as durability, size, and waterproof quality of the card as a benefit over the existing citizenship card. They did not mention legal identification, public welfare service delivery, or national security benefits that the government has amplified as benefits. The cost-benefit privacy framework of individuals willing to give up personal data for perceived benefits[22] does not hold water in this case as the end-users were simply unaware of the official benefits. Neither has there been the notion of informed consent.

> *"They just said that it was mandatory to get registered and they will face difficulty in the future if the people with citizenship won't fill the form. They did not explain the benefits and usage." End-User 12*

However, a senior official with the DoNIDCR asserted that information about the project and enrolment was disseminated using multiple media, and noted:

> *"Panchthar was the first district to start the registration for the NID card so, at that time, the locals were informed through local FM and ward offices. Also, we personally requested social institutions and organizations to inform the locals about the process, required documents, and other information about the registration process. We also used local mass media channels – FM radio, newspapers, pamphlets were distributed to inform the people." Government Official 01*

The end-users did not mention any of the above-quoted media channels. Their sources of information came mainly from family members, neighbors, friends, and trusted community members. Some of them also mentioned that local municipality officials and data collection operators provided some information at registration centres.

We also found that female respondents were more dependent on male members of their family such as their father, husband, brother, and/or son for information about the NID program. They also found it difficult to make time to attend registration camps that are held for a limited time in their wards as women have almost full responsibility for most domestic chores as portrayed in Case Study 1. If they miss that window, it becomes doubly challenging to find someone to take them to the Chief District Office (CDO) office later. This suggests that they did not have direct access to official information and received a word-of-mouth understanding of the NID card's registration procedure, its uses, and benefits.

### *Case study 1*

(Case Study names have been replaced by pseudonyms)

Shanti came to know about the local registration camp for the NID card through her friend. She heard that one has to register for this card because

[22] (Alessandro, 2019)

the citizenship card would not be useful in the future and this card will be used for every service. Her husband also informed her that both husband and wife should go together to register for the card with their citizenship and marriage certificate but that the registration process would take a long time.

Her friends went to register but she could not find the time because she was busy with household chores. She was also unable to coordinate the time with her husband to go with him to register. At that time, she thought that she would be able to register later so she did not worry too much about missing the registration due to her household chores.

Shanti would like to register now but she is not sure if she can since the registration camp has moved from her ward. She has no idea where she should go to get information about the next available dates to register in her ward.

The above examples highlight how women in rural and semi-urban areas are dependent on men for their information and also to escort them to register. They also face additional challenges of time, since the burden of domestic chores falls entirely on them. This often leads to them not being able to register or having to make extra arrangements due to time constraints or having to travel long distances to the CDO to register.

## Contradicting Information

Government officials asserted that the computer operators, selected from a vacancy notice, were well trained about the registration process using digital equipment, and knew how to secure data before being deployed to the registration station.[23] However, the data collection operators questioned the clarity of communication they had received and one of the respondents noted:

> *"The National ID Card Act wasn't passed and we had started work while the communication was still not clear. If someone would come and ask for details, we didn't have clarity on where the card will be used and how. We relied on the information we knew." Government Contracted Data Collector 01*

The interviews revealed that some of the contracted operators were school teachers, who were not able to attend the training because of their teaching jobs. This could have resulted in uneven training of operators with some of them relying on word-of-mouth information from the other operators before going out into the field. The data collectors are the front-line sources of information for end-users at registration stations; their incomplete knowledge initiates a cycle of confusion.

The difference in accounts between government officials, contracted data collection operators, and end-users suggests an information gap in the communication strategy that has led to overall confusion. The lack of credible and complete dissemination of information at the grassroots level continues to be a challenge that the government needs to address. Town hall type of programs should have been initiated by the DoNIDCR at urban and rural municipalities

[23] Registration Station - place where the mobile team was conducting the registration for NID in the Districts.

to include consultations with multistakeholders during the planning phase so that official information about the NID card is well disseminated and multistakeholders' opinions are taken into account.

Our findings suggest that government officials, multilateral agencies, and private sector representatives tend to push the development and efficiency narratives about the benefits of digital ID cards over effective communication of policy information or the registration challenges faced by end-users. The development narrative was limited to economic prosperity and a narrow and naive idea of law enforcement, as exemplified by the remark of this government official:

> *“If I go to any institution to take any services, then I can show that card to prove my identity as the eligible consumer. Also, the service provider should provide services to me only after checking my card. And let's say, if I commit any crime then that card can be used to know about my real identity.” Government Official 01*

These narratives about benefits have always been at the center of government projects. The NID is introduced as a tool to provide services to citizens intended to benefit the service-seeker. However, it is crucial to examine whether the service seeker really benefits from these projects (as promised by the government) or not. Do these services in fact benefit another agenda? It has to be examined whether such projects might exclude marginal groups who do not fit into government ‘identifiers' but who are supposed to be eligible to receive benefits promised by the state.

In a context where it is not clear what the NID's function is, one has to question the relevance of this program. The sharing of information being limited, incomplete, and haphazard without proper planning and mapping could be a strategic move by state institutions to collect large amounts of data from the public.

## Confusion between the NID card, the citizenship card and India's Aadhar card

The majority of respondents including government officers at the municipal level do not seem well-informed about the use of the NID card vis-a-vis the existing citizenship card. People were not sure about the timeline for when the NID card would be used or what would happen to the citizenship card once the NID card was implemented. The quote below from an end-user illustrates the confusion:

> *“In the beginning, I heard from everyone that one has to get the NID card because it will replace the citizenship card in the future. It will work instead of the citizenship card. But the citizenship card is still required for government services.” End-User 03*

Not surprisingly, the official from the DoNIDCR was the only respondent who unequivocally mentioned that the NID card will definitely replace the citizenship card in the future for both government services and ID purposes. However, at the public meeting that we attended virtually, the Director-General of the DoNIDCR in response to a participant's query about both the cards noted that the citizenship card would continue to exist as a political document. He did not clarify what exactly he meant by ‘political document'.

The final layer of misinformation that our study revealed was that most end-users and some government-contracted computer operators were comparing the NID card with India's Aadhaar card. The major difference between the NID and the Aadhaar card, which they were unaware of, is that Nepali citizenship is mandatory for registering for an NID card, whereas the Aadhaar is a foundational identity document based on a minimum of six months of residency in India before applying for it.[24] The Aadhaar is not a proof of Indian citizenship.

The comparison was made primarily concerning getting food rations which is just one of the government service deliveries that the Aadhaar is linked to. Responses from end-users and government officials include the following:

*"Even people who did not understand said that this card will be similar to the food ration card in India. I have not thought about it. Maybe we can get rasan [rations] in the future." End-User 21*

*"We hear that the NID card is based on and similar to India's unique ID Aadhaar card. I think the NID card is very important. If someone missed registering, they must register." Government Official 02*

The probable reason behind these comparisons could be because our field study was conducted in Panchthar and Jhapa districts which are close to the Nepal-India border and the residents in these districts were familiar with the Aadhaar card in India.

Unclear information and misinformation about the NID card, primarily among end-users, from registration to awareness of benefits, suggests that it has not been a priority of the government to provide correct information on the NID to citizens. A clear communication channel where people can collect relevant information is missing.

The second major thematic finding addresses the aspects of digital privacy and information security concerning the NID. The following section presents our findings related to these issues in greater detail.

## Privacy and security

Digital privacy and information security are foundational concepts linked to national digital IDs and have a profound impact on citizens' overall digital rights. This also includes the right to information, the right to access knowledge online, the right to protection and security of sensitive data, and the right to informed consent. None of these were explained to grassroots end users during data collection for the NID card.

## Digital privacy and information security

Digital privacy concerns are often brushed off as a 'western' concept by South Asian legislators and policymakers and they comment that in close-knit Asian communities people share their most private details with one another.[25] What they miss is the element of trust that individuals often share with their close-knit communities of family members and neighbours. They assume that individuals will repose the same level of trust in the state. This is a fallacy because studies have shown that globally people do not trust their personal data with governments and private corporations.[26]

In this study, though, the end-users may not have had an understanding of terms such as digital privacy or biometrics, they intuitively understood the risks of sharing private information and data breaches, as exemplified in this response:

*"Private information should neither be asked by the government nor given by the individual. The data can be leaked anytime and it will*

[24] (Aadhaar Dashboard, 2019)
[25] (Manzar, 2017)
[26] (Chakravorti, 2018); (Anamitra et al., 2017)

*be difficult if people's private data is leaked." End-User 27*

Private sector and multilateral agency representatives were also concerned about data privacy and the collection of inordinate amounts of citizens' personal data in case of misuse or data breaches. An interviewee from a multilateral agency also shared that there is an ongoing effort to collect data by different government institutions at the local level along with the NID program, often duplicating the kind of personal information collected. They noted that it is often the practice for governments to collect more data than is required, in case it can be used in the future, without any regard for data minimization or proportionality which are global standards of mass digitization programs.

This also raises questions of informed consent if the government is collecting massive amounts of personal and sensitive data, without explaining why. While multilateral agencies promote legal identification via digital ID systems as an inclusive development tool[27], those we interviewed for this study were cautious about what data is shared and with whom. One of them noted:

*"The government will now have to decide what kind of data can be accessed by whom or else there might be a violation of rights of people as it contains sensitive information. For example, data of property of an individual." Multi-Lateral 02*

Government officials, however, tended to place more emphasis on the efficiency of use and capacity of surveillance with the NID card's database that could be used for public service delivery, national security, and law enforcement purposes than on the privacy rights of Nepali citizens, or the harms related to possible data breaches. As one official noted:

*"Every sector that would provide services including in the private sector, like a bank which is allowed by the Government of Nepal, as per the law would be able to access basic information of the NID card. Their system will be connected to our VPN and the data will be integrated with it to access basic data and verify identification."[28] Government Official 02*

During the registration process, Nepali citizens were not informed about the government's plans to link the centralized database with other public and private organizations to improve efficient delivery of services.

It is also problematic when policymakers assert that end-users voluntarily share data in return for the convenience of accessing goods and services. There seems to be an 'illusion of voluntariness' that policymakers refer to where those who choose not to register are punished by not being able to access public and private services including government welfare, banking, insurance, vehicle registration, mobile connections, etc.

Government officials were the only stakeholder group that had full confidence in the security protocols adopted by the DoNIDCR to maintain confidentiality, integrity, and availability of the data stored in the central repository even if the data is shared with other organizations.

Their responses were also contradictory because while they accepted that the possibility of a data breach cannot be denied by a hundred percent, they also claimed that it could not happen in Nepal because they had adopted cybersecurity systems similar to the ones used in the United States and Europe. This argument is fallible as we have seen how central and sectoral government databases in the United States and Europe-

[27] (World Development Report: Enabling Development - Digital IDs, 2016); (ID2020 Summit 2016 | United Nations Office for Partnerships, n.d.)

[28] (Chautari, 2022)

an countries have been hacked in the last decade with incalculable harm to the organizations and the individuals whose data have been breached.[29] Even a country like Estonia, which is viewed as a good example of e-governance,[30] has faced several hacking incidents.[31]

In addition, when the authorities were asked about the security of people's data, their responses gravitated to national security. They claimed that given the physical server for the NID is situated inside Singha Durbar and not anywhere outside of the country, it is a secured system. This venue apparently provides the psychological notion of 'national security' – Singha Durbar being a palace built during the Rana Dynasty that now houses ministries and public offices in Kathmandu.

An increasingly digitized world is also one where geopolitics and warfare have entered the cyber domain and government databases are more regularly being used as targets by state-sponsored proxy actors to destabilize nations.[32] This should give Nepal's policymakers pause to reconsider their rushed approach to centralized databases and include civil society organizations and security researchers to present their perspectives as is being recommended globally.[33]

Both private sector and multilateral agency representatives were concerned about the information security of large centralized databases and were critical of the inordinate amount of data being collected for the NID card and recommended that the government should follow the premise of data minimization by collecting only data that was required for digital ID purposes. Private sector interviewees were also concerned that the centralized data centre was managed by a private multinational — Oracle Enterprise — rather than also having a government-run Cybersecurity Emergency Response Team as found in other developing countries.

At the ground level, most end-users were not able to understand how to set up basic Personal Identification Numbers (PIN), or were unable to remember them, especially those with minimal formal education — data collection operators had to set the NID card's PIN for them and then shared these PINs with local representatives. The undernoted responses by some of the data collection operators highlight just how fragile the information security system is because end-users with low levels of digital literacy do not understand the sanctity of secret PINs:

*"When we distributed cards in Panchthar, we were not able to explain to people why we need the PIN. Especially those who are illiterate. Some aren't able to remember the PIN code and some didn't know what to put. So, the operators had to put the pin code ourselves. We didn't have proper instructions. Some put four ones (1111) and for some, we put their year of birth." We also notified the local representatives of their constituency's pin code." Government Contracted Data Collector 01*

*"…in villages, it's mostly elderly people, so they can't remember the number. In the cards I distributed, I used their year of birth." Government Contracted Data Collector 02*

Not sharing one's PIN is one of the most basic ways to protect one's data. Sharing a PIN allows one's data to be misused by others and directly compromises the privacy of the individual and the information security of the system.

[29] (Mathews, 2021)
[30] ("Success Story – Estonia's 20 Years of Digital Transformation – The Digital Republic," 2020)
[31] (Paraskevopoulos, 2021)
[32] (Lisko, 2014)
[33] (Buzasu, 2020); (Handa, 2016)

The data collectors too were confused about what data breaches of centralized digital databases meant and suggested that a manual record be kept along with the digital database that should be kept securely, as seen in the following response:

> *"If something like hacking or stealing happens and if we lose the data or the data gets deleted, then, the manual documentation will be very important and it will have to be kept very securely." Government Contracted Data Collector 03*

Since the operators are collecting very sensitive biometric and demographic data from Nepali citizens, not having received adequate training raises critical concerns with regards information security. It also highlights the rushed effort by the government to push the scheme without the fundamentals being put in place first.

The NID guidelines make it clear that there are plans to share the database with authorized public and private sector organizations for ID verifications and service delivery. While the DoNIDCR officials were confident about the level of information security of the central data repository, it still remains unknown how other government agencies, private organizations, and development-related NGOs will store and use this data.

Nepal's existing Individual Privacy Act is simply not enough for the gamut of data protection issues a digital era needs. The legal provisions are not sufficient to safeguard citizens' rights in the event of a data breach. The government's ambitious plans for a Digital Nepal Framework must include legislation for online data protection, digital privacy, and information security.

Rather than being informed or aware of critical digital privacy issues or information security concerning the NID card, most end-users were misguided into thinking that possessing the card was a form of 'true Nepali' citizenship. The next section reveals how a nationalist ideology has been placed by end-users on the NID card and how this can foster other forms of socio-structural 'othering' that prevails in Nepali society.

## Privacy vs. safety and security

The contracted computer operators felt the NID card program will help to identify criminals through surveillance capacities inherent in the NID card's demographic and biometric database.

Connections are often drawn between giving up personal privacy for safety and security to protect citizens such as in post 9/11[34] narratives where American citizens willingly parted with personal liberties to control terrorism. They too assumed the US government would never use surveillance or negatively profile its citizens. However, Snowden's[35] exposure of widespread and extra-judicial mass surveillance by the US government on its citizens is a case in point. It revealed how unchecked mission creep of government digitization programs can occur due to these false narratives of security and surveillance.

[34] On September 11, 2001, suicide bombers hijacked American passenger planes in United States and flew them into the twin towers of the World Trade Center in New York, causing thousands of lives to be lost, a day that is remembered as 9/11.

[35] Former CIA official Edward Snowden, while working for the American National Security Agency, revealed that the American government/agency was secretly collecting personal phone records, internet usage, and other private information of influential figures, which included American citizens and foreign leaders. Due to this revelation, Snowden had to go through a life of exile. His actions were considered as an anti-patriotic act by some, while others viewed it as an exposure of government surveillance and violation of human rights.

On the other hand, end-users are asked to choose between privacy and safety — it could be argued that this is an unfair choice. For privacy and safety to coexist, the infrastructure should be designed accordingly with clear intention. The government does not seem to be concerned about privacy in the case of the NID.

## Biometric data and breach of privacy

Biometrics-based programs have become the aspirational technological tools in South Asia's massive digitization projects that portray a certain level of development. They are always presented and implemented as efficient, inclusive, neutral, and anti-corruption innovations without any thought given to how they impact all stakeholders, especially those at the margins[36] and the socio-economically weak.[37] They tend to ignore the numerous studies that have been done that point to how biased, exclusionary, and not so efficient these technology solutions are.[38] Policymakers often undermine the fact that these technological solutions are also a new form of bureaucracy and come with both pre-existing and new complications of large bureaucracies.[39]

Despite low levels of digital literacy among Nepalis, there was no strategic communication plan to share with the end-user the kind of biometrics data being collected and possible implications of such data being generated. Over sixty percent of the end-users we interviewed were not familiar about the concept of biometrics and that it entails giving away some of their most personal and sensitive bodily data. Most women and elderly respondents mentioned the details of only demographic data being collected and a photo being taken. Others remembered other aspects without knowing that this was biometric data and unique to their bodily selves. They were not informed why the different points of biometric data were being collected for the NID card, hence there was no real informed consent. These responses from end-users illustrate their lack of knowledge:

> *"No, I did not have any information about why such information is being collected. The staff also did not mention anything because it was crowded that day and there was a long queue as well. I also did not ask anything because they were busy with registrations."*
> *End-User 04*

Biometric data is the most personal and sensitive data of an individual since it has to do with their physical body including fingerprints, iris scans, photographs, DNA samples, etc.; it has critical implications for a person's privacy and other bodily and digital human rights. The misuse of biometric data oftentimes results in the targeting of vulnerable and minority populations for political agendas, and data breaches can have existential impacts on the lives of individuals. The end-user response above shows the almost non-existent process of informed consent, which also reveals policy makers' perception of people's choice and autonomy.

## Nationalist ideology and government accountability

Most end-users saw the NID card as a confirmation of them being a 'true Nepali' citizen rather than viewing the card as a form of personal identification and to access public

[36] (Digital IDs Rooted in Justice: Lived Experiences and Civil Society Advocacy towards Better Systems, 2022)
[37] (Khera, 2017)
[38] (Lohr, 2018); (Khan & Roy, 2019)
[39] (Fluri et al., 2015)

services more easily. We have divided this section into two sub-sections to discuss two issues that emerged from this notion of being a 'true Nepali'; first that of a narrowly defined nationalist ideology and second, the accountability of the government.

## Nationalist ideology

We found that one of the main reasons that most of the end-users were registering for NID cards was because of a narrow nationalistic ideology. Respondents from both districts believed that the NID card was a matter of national pride and this identity was only given to 'true Nepali' and 'pure Nepali' citizens. As one end-user remarked:

> *"The moment you mention NID card it is linked to nationality. It is the supreme proof of the identity card of Nepal and you always feel proud about it." End-User 02*

This narrow nationalistic fervour is also troubling because of the prevailing 'othering' that happens between different ethnic groups in Nepal with the Madhesis (people from the plains, Terai area of Nepal, closer to the India border) being socially discriminated against and not considered 'true Nepalis' by those from the hills with lighter colored skin and different facial features.

The narrative of nationality based on homogenous ethnicity and labelling people from different ethnicities, particularly Madhesis, as being a threat to national sovereignty is detrimental. The Madheshi people are already considered second-class citizens and denied a 'true Nepali' identity due to differences in ethnicity and language. The discriminatory provision of waiting for seven years for Nepali citizenship when a foreign woman marries a Nepali man has specifically placed married Madhesi women in a vulnerable position of being stateless as cross-border marriage is a common phenomenon in Nepal.

If the NID card further exacerbates this 'othering' of regional ethnic groups based on a narrow definition of nationalism that they associate with the NID card, it will increase the social exclusion of these groups as shown by Case Study 2, below. It is also within this context that information about the NID card should be made clear and credible.

End-users also expressed that the NID card will reduce citizenship fraud, mentioning in particular people from India. This may also be reflective of the ongoing anti-Indian sentiment that is prevalent in Nepal.

> *"I do not know much but, from my understanding, we are closer to the Indian border and there are cases of people having citizenship from both India and Nepal. So, it will stop such incidents." End-User 20*

Government officials and data collection operators also placed heavy emphasis on fraudulent citizenship documents and linked this to national security as well. They too mentioned the open border between Nepal and India, reflecting anti-India sentiments, along with the perceived risk of 'Indians coming to Nepal' and 'getting multiple identity cards to access government services.'

### *Case study 2*

Rewa is a 28-year-old resident of Jhapa district. She has been living in Jhapa since birth and never had a citizenship card because her father did not have one. According to her, her father died in an accident a long time ago, and had never applied for a citizenship card. Although her father's death was registered in Jhapa, she was told that she couldn't apply for a citizenship card based on her father's death certificate. She bemoaned the challenges she faces because of this and expressed her frustration at the system, saying: "Where will I bring the citizenship of my father from? My father was swept away in the river — shall I jump in the river to make my citizenship?" This also meant that she was unable to register for the NID card. Even though a citizenship card is not a prerequisite for the NID card according to law[40], in practice it is. Her neighbours had also informed her of the same, so all except her from her ward went to register.

Despite her willingness to do so, and having supporting documents proving her identity as required by law, Rewa was not allowed to register for the NID. She feels helpless and angry about being excluded from registering and from the services to be provided by the NID card.

Rewa's case study provides an insight into the many challenges that people face at the ground level with policy regulations that assume that mandatory pre-requisite documents are easily available to all people. NID policymakers must make provisions for such cases if the card is to be inclusive and benefit everyone.

## Government Accountability

A significant number of respondents were not critical or questioning the government about the actual intention of the NID. This lack of questioning in government apropos large-scale digital policies is often misplaced due to low levels of digital literacy and a lack of understanding of the critical implications of such policies. In addition, although it may look like people trust the government, we need to understand why there is no choice for people to decide whether they want to register or not. The power of the hierarchy is quite evident. The following representative responses underscore both trust in government and low levels of digital literacy.

*"Perhaps the government will not attack its own citizens and misuse our information. Even if that happens, it may not be just for a single individual. So, I think something like that will not happen." End-User 20*

*"The government might have protected it well. If in case the data are hacked or stolen there are not many important data in the card." End-User 04*

Private sector and multilateral representatives were more skeptical about the efficiency and accountability of the government for the implementation of the NID card. One of the private sector interviewees noted strongly that people working in government bureaucracies "do not take any responsibility for their work and the lack of accountability in government will hamper the implementation of the program as well". Another private sector respondent noted:

*"The most important bit is implementation and execution. When can we show the result after execution? What is the timeline? I haven't seen clearly what the projection and Plan*

[40] National Identity Card and Registration Act, 2076, Section 9(4) states that persons who have a citizenship will be provided the identity card according to their citizenship whereas those without a citizenship card but are eligible for one will be provided an identity card as per the provided proofs.

*of Action are for this NID project." Private Sector 01*

The next key finding from the study was concerning the potential for exclusion of certain groups that could occur due to several factors such as malfunctioning devices to digital divides, and gender. Some of these issues, such as faulty devices and gender, have been referred to earlier but they will be discussed in the next section with the context of the potential for exclusion.

## Exclusionary by design

While we question the relevance of programs such as the NID, given it is rolling out rapidly in the country, there is an urgent need to also look into issues of exclusion and the harms associated with it, especially concerning those already marginalized.

Global research has repeatedly found that existing marginalized and vulnerable population groups face a greater potential for exclusion from digital ID systems than they did in physically networked close-knit communities. This is especially true in countries similar to Nepal where digital IDs render large swathes of undocumented population groups, stateless. They often do not have prerequisite documents that enable them to register for a national ID such as birth or marriage certificates, citizenship cards, passports, etc.[41] Globally, CSOs advocate for and work with these population groups on other social equity issues; this is an important reason why CSOs should be included in multistakeholder consultations for national ID programs so that they can represent the obstacles to registering faced by these groups and prevent them from being excluded.

## Pre-requisite Documents

Government officials admitted that some people without all the prerequisite documents had been excluded from registering for the NID card. These included the following groups of people according to findings from our interviews:

- Internal migrants who did not have a migration certificate and were unable to get a recommendation from the local registering unit.
- Married women and men who did not have a marriage certificate.
- Some married men who worked abroad registered as unmarried as they did not have the time to secure a marriage certificate.
- Older Nepalis without citizenship cards.

*A local data collecting operator stated: "I think around 20% have missed the registration. Many were not interested. Many did not come to get their photos taken and said they'd register later rather than now because of the crowd during a pandemic." Government Contracted Data Collector 02*

One of the multilateral agency interviewees also stressed that the government would need to clear up the confusion with the citizenship card being considered a requisite for registering for the NID card. Some end-users also mentioned that elderly people whose citizenship card was old and damaged could not register as they had to travel to the district headquarters to make another copy of their citizenship card. Most of them chose

[41] (Digital IDs Rooted in Justice: Lived Experiences and Civil Society Advocacy towards Better Systems, 2022)

not to register for the NID as they were old and not expecting any services from the card.

Despite finding so many cases of exclusion and the potential for exclusion in this limited pilot study, the director-general of the Department of NID Card and Civil Registration said:

*"Right now, no one is excluded. Everyone who has a citizenship card is included in the registration process." Government Official 02*

This reveals another level of disconnect between policymakers, local government data collection operators, and end-users on the ground. It continues to highlight why multistakeholder consultations are required to plug the gaps between policy on paper and policy in practice.

## Gendered program

Women respondents noted that they were also dependent on men in their families or male neighbours to access information related to the NID and to even go to the registration centre itself.

Women tended to be excluded more because of the prerequisite document of a marriage certificate to prove their place of residence. Marriage registration is not common in many rural areas and some women in rural areas are separated from their husbands without any legal procedures. Other older women have never had a marriage certificate. Marriage registration certificates and proof of relationships were compulsory for married people; some women were excluded despite having valid citizenship cards. As a digital rights organization that examines the space through a feminist lens, we were not surprised by this as it reconfirms findings from our previous research, Identities Experiencing the Internet[42]; that women experience the digital world differently and often get excluded from certain digital spaces.

Many women respondents mentioned that if the marriage is inter-district then they were allowed to register only if they had marriage certificates or relationship proof from their husband's district. It became impossible for many married women to register because either their husbands were abroad and they could not apply for a marriage certificate or they were living separately from their husbands, or their husbands had abandoned them. As one of them stated:

*"Some people who had inter-district marriages and people without marriage registration certificates had some difficulty registering. They had to first make a relationship certificate as proof, and then only could they register for the card." End-User 12*

*A government computer operator also shared how those without marriage certificates could not register people for the NID card:"Some people did not have marriage registration certificates but said they were married. If they were asked to bring the registration certificate, they would say they did not have it. So, their registration would get rejected." Government Contracted Data Collector 03*

We have placed marital status as a gendered difference because men and women experience the requirement for a marriage certificate to register, differently as showcased in the Case Study 3 below. While it is true that both men and women require marriage certificates to register, we learned that men who did not have a marriage certificate and found it difficult to get one at short notice, registered for the NID as unmarried. We are not sure how men were able to do this, but our grassroots work with women suggests

[42] (Kayastha & Mamata, 2020)

that married women live in their husband's homes, and in a patriarchal society like Nepal they find it difficult to falsely claim unmarried status. Other than a gendered difference, this also points to another issue of 'dirty data' being included in the database with incorrect information.

***Case study 3***

Maya, a 42-year-old Dalit woman, is an elected ward member of Panchthar district's municipality office. She was born in Panchthar district and her citizenship card (a required document to register for the NID card) is also from there. However, Maya is married to a man from a different district and her marriage certificate is from her husband's native district.

When the NID registration mobile team came to her ward she was excited and worked as a volunteer helping people in her ward to register by filling up the form and verifying their documents. She wanted to register in Panchthar district, where she was born and has been working as an elected member of the community. But the NID regulations did not allow her to register from Panchthar because her marriage certificate was from another district. She informed us of her situation and her disappointment in not being able to register from Panchthar, saying:

"I have my citizenship from Panchthar, I'm an elected local representative and a responsible citizen of Nepal but I feel sad and feel like I am no more the citizen of Nepal because I was not able to register from Panchthar district."

She requested other local elected representatives and also went to the office of the CDO to ask for help to allow her to register for the NID card from Panchthar district. She was not allowed to register.

Maya was informed about the ongoing registration at her husband's home district on the last day. She had to travel a long distance to get registered from there and reached the registration centre late in the evening when they were ready to close. She was fortunate that the officials were considerate and allowed her to register after she explained her situation to them. While she was glad that she was able to register she was disappointed that she could not do so from Panchthar due to her marital status.

We can only imagine how many other women have faced similar challenges, without Maya's access to government officials, a smartphone, or the ability to quickly travel to their husband's district to register.

The mandatory regulation for married women to get registered from the district where their marriage certificate is issued underscores the gendered difference that they face. It also poses critical questions about the potential for exclusion for those women who identify as married but do not have a marriage certificate because of distinct reasons.

From access to information to the logistics of getting to a registration centre to additional challenges of pre-requisite documents for married women, the above section highlighted the challenges faced by women. We would urge policymakers to consider these gendered differences to ensure that public digitization programs like the NID card do not leave Nepali women behind.

## Ableism in the system

There is the potential for exclusion of people with disabilities (PWD) because of the mandatory inclusion of biometrics. The biometric data collected consists of fingerprints of ten fingers, digital signatures, iris scans, and digital photos. There is a probability of complications in identity authentication if any person with a disability has missing fingers or eyes or who cannot provide a digital signature. This would create further difficulty to access services through the NID card, especially for PWDs.

We interviewed some PWD end-users who mentioned that it was also difficult for them to go to the registration centre and complete the registration. As one end-user commented:

> *"It was tough for people with a disability like us. The registration centre was on the first floor and it was difficult to reach the first floor." End-User 25*

Furthermore, Nepal is a predominantly agricultural economy where the majority of the population is engaged in crop or livestock cultivation. Fingerprints of agricultural workers often erode due to heavy manual labour thus fingerprints are not accurately recorded during biometric data collection. Our field research also revealed that people with disabilities or less than 10 fingers were not able to give their fingerprints. The devices recorded both these groups as 'damaged' and show an ableist perspective of collecting biometric data.

## Cost of unplanned digitalization

Government officials often tout the multiple points of biometric data as a way to overcome existing bureaucratic challenges, however, it has also been found that malfunction of biometric authentication devices at the point of service delivery, with no electricity or internet connectivity in rural areas, or incomplete biometric information has meant these people lose their access to goods and services linked to digital ID systems.[43] The most severe form of this was recorded with food rations in India, where some people in villages died of starvation because their biometric information on their Aadhaar card could not be authenticated at government ration shops and they could not get their food rations.[44]

The digital divide and the uneven internet infrastructure in Nepal creates immense potential for exclusion in rural areas where connectivity is unreliable and expensive. How will these populations access NID-linked government services if they are unable to verify or authenticate their identity digitally? The premise of biometric digital ID cards is based on digital verification and authentication of identity. If these populations have to rely on a physical card to prove their identity, all the arguments by the government of stopping the use of fraudulent physical ID cards, deduplication, and stemming leakages in the public service delivery

[43] (Digital IDs Rooted in Justice: Lived Experiences and Civil Society Advocacy towards Better Systems, 2022)
[44] (Khera, 2017)

systems through the NID card do not hold much water.

Not surprisingly, private sector stakeholders from Kathmandu are confident that the level of internet connectivity in urban areas will make it easier to implement NID without any concern for rural connectivity challenges. Private sector interviewees also expressed that the pandemic was an 'opportunity' for them to extend services through the online medium and perceived it as leading to the greater social good. The pandemic which affected the daily lives of so many Nepali people, especially from marginalized communities, was seen as an opportunity by the corporates, and the 'development' narrative for them was limited to economic prosperity alone.

Furthermore, other kinds of digital divides based on gender, class, education, ability, and digital literacy levels continue to exist in Nepal apropos access to the Internet. These intersections continue to impact how different groups access the benefits of internet-enabled services. Marginalized groups with restricted access to the Internet are often excluded from digital spaces to express their experiences.

## Logistical exclusions suggestion: Geographical exclusion

In Panchthar, we found out that it took citizens only one day to complete their registrations. But our respondents from Jhapa mentioned that it could take a minimum of two days to register due to understaffing of registration centres resulting in long queues. Many people did not go back to the registration centre because they had to stand in line for 2-3 days just to acquire a form and then they had to stand in line again for another 1-2 days to be registered. These repeated trips to get registered also resulted in some of them missing the registration deadline in their area as expressed by the following response:

*"I had to go for two days to register. I had to stand in a queue in the morning and go here and there for registration. People standing after 25 people in the queue were unable to register on the same day. They would close the registration centre in the daytime." End-User 23*

Private sector interviewees from Kathmandu reconfirmed the experiences of end-users in Jhapa. Similarly, local government data collectors also sympathized with end-users who often had to travel long distances to get registered and this meant the operators had to work beyond their official hours to accommodate them.

*"When we are in the field, people travel for hours to get to the office. So if they had walked for 4-5 hours and they couldn't get registered, we would consider registering them on humanitarian grounds. We have worked from morning till late night from 6 a.m. – 9 p.m." Government Contracted Data Collector 01*

Logistical challenges of multiple trips to register for the NID card also meant that some end-users did not return and were excluded. If the NID is to be inclusive the registration process needs to be simplified and access made easier for all.

# Conclusions & Recommendations

As a civil society organization working in the digital rights space, the most striking learning from this study was the complete absence of active civil society participation at national digital policymaking spaces. Our interventions tend to be reactive after digital policies are in place, even though our reports describe and inform readers about ground-level digital and online experiences of vulnerable groups. Secondary research for this report about how other civil society organizations in developing countries have engaged in advocacy reconfirmed that our advocacy for justice and rights-based frameworks for national digitization policies need to be proactive, collective, and organized so that we take a seat at the policymaking table from the beginning.

Secondly, we are hopeful that Nepal's policymakers will acknowledge that such mandatory national digital ID systems that collect inordinate amounts of personal demographic and biometric data of citizens must have water-proof governance and accountability protocols to protect the human rights of individuals, especially those from marginalized communities. For instance, Nepal's NID card duplicated itself with other data collection initiatives at the state and municipal levels and shared centralized databases with public and private sector organizations in a manner that a leading digital rights organization, Access Now, calls a 'heedless collect-it-all or link-it-all approach.' These approaches pose unnecessary data privacy and information security risks for those whose data is collected and shared. We recommend the government of Nepal to adopt fair, accountable, and transparent digital policy processes that embrace multistakeholder consultations and carry out regular impact and risk assessment surveys of these policies.

At the very least, Nepal's policymakers must ensure that legal safeguards and requisite laws are revised to plug loopholes and clarify ambiguous exceptions to protect such data and minimize its extra-judicial use. Along with strict governance standards, the government must adopt a strategic communication policy that informs credibly and completely all aspects of the program to prevent misinformation.

While we appreciate and understand the benefits of using technological solutions to increase public service delivery mechanisms, private sector identity verifications, and stem leakages and corruption of existing service delivery mechanisms, we also know from our work with grassroots and vulnerable communities in the online space that some deep-rooted socio-cultural structures marginalize them and their challenges. These social barriers require more contextual and nuanced interventions for their upliftment and inclusion. It has been found that biometric-based digital IDs tend to exclude such groups rather than include them. Therefore, we strongly recommend that the government not exclude people from services regardless of possession of NID.

Moreover, corruption and crime are complex and rooted in structural social issues of asymmetrical power relations between government bureaucracies and citizens, poverty, uneven economic development, and unplanned urbanization. Trying to solve such complex social issues by using technology might only divert attention from fixing the root causes of these problems and can validate surveillance in the hands of state and corporations.

Based on the findings from this study and best practices learned from other global studies about digital ID systems — particularly in Global South countries — we provide two sets of detailed recommendations for action as Appendix C. The first set of recommendations is for civil society organizations and researchers. The second set of recommendations is for our policymakers to adopt a framework that includes adequate attention to accountable and transparent procedures and governance, data protection, digital privacy, and information security.

In conclusion, we appeal to all readers of this report to engage with us on any issues we may have missed, so that together we can build a digital Nepal that is safe, just, and fully representative of all citizens.

Note: Detailed set of Recommendations for Action as Appendix C.

# Appendix A: Research Methodology and Methods

Since this was an exploratory pilot study and to our best knowledge, the first one to map end-user experiences with the NID card, we purposefully chose to use a qualitative methodology which is preferred when researchers have minimal information about the subject and the objective is primarily to describe social phenomena.[45] We also wanted to collect culturally and contextually rich primary data that provided granularity and nuance about how citizens were experiencing the national digital ID card in Nepal.

Our primary research was designed to use ethnographic methods of face-to-face, in-depth, semi-structured interviews but the next wave of COVID-19 struck and we were forced to use telephone calls to conduct interviews. The following section on conducting qualitative research during a pandemic will provide more detail on the opportunities, challenges, and ethical considerations we faced. We simultaneously collected secondary data by doing a close read and analysis of textual materials found in the public domain such as the NID program's website, relevant policy documents, and media reports to gain a better understanding of Nepal's NID card details, as well as global research that has reported on other country experiences with digital ID card systems to be able to place the Nepal experience within a global context.

Our sample population of interview respondents was from the districts of Panchthar, Jhapa, and Kathmandu (since the NID department is located in the capital). For data collection, both rural and semi-urban municipalities were included. In Panchthar, Phidim municipality and Yangwarak Rural Municipality were part of the field study. For the district of Jhapa, Mechinagar Municipality, Kachankabal Rural Municipality, and Baradarshi Rural Municipality were included. The idea of selecting the other two districts from different demographic regions was to understand the perspectives of end-users from hilly and plain terrains, urban/semi-urban and rural areas, as well as those close to the international border with India which experience some migrant populations on both sides. The breakdown of the sample population is included in Appendix B.

While our study sought to examine the experiences of primarily end-users, our research design also included a limited number of interviews with government officials and government-contracted data collection operators, private sector representatives, and representatives from those multilateral agencies that were involved during the initial planning and piloting of the NID card. In total, we conducted 43 interviews — 31 end-users, 7 from the government, 3 from the private sector, and 2 from multilateral agencies.

We used local interlocutors from the two districts of Panchthar and Jhapa to select end-users who had registered for the card since the study was about mapping the experiences of those who had registered. Also, the use of local interlocutors is an accepted practice in conducting qualitative field research when the researcher is unfamiliar with the local community and uses a trusted member to help identify participants.[46] We conducted a one-day workshop with the local interlocutors to brief them about the research and the sample population of end-users we wanted to interview based on our research design. Despite our best efforts, there was some miscommunication about

[45] (Baxter & Jack, 2015)
[46] (Baxter & Jack, 2015)

the selection of a few participants that we were able to correct through telephone calls with the interlocutors.

As recommended when conducting semi-structured interviews, we used an interview protocol to guide our interviews with the different stakeholder groups.[47] The interview protocol included sections on the registration/enrolment, updating, and distribution of the card, the uses and benefits of the card, biometric data collection, data protection, digital privacy, and cybersecurity. The final section was left open for any other information that the respondent wanted to share about their experience with the card. Please note that the interview protocol was used as a guide to asking questions about the issues and not used ad verbatim.

The interviews were conducted in Nepali through voluntary participation and completed between 13th May 2021 and 2nd July 2021. All interviews were recorded with the full permission of each participant before we started the interviews. Participants were provided with a brief background about the study. The audio recordings were transcribed anonymously and then translated into English. The English translation was done because the final report would be published and promoted online in English for wider global reach. With the growth of digital NID systems globally, policymakers, NGOs, think tanks, academics, and multilateral agencies have shown keen interest to understand country-level experiences.

Transcription was followed with a close read of all the interviews multiple times to arrive at some thematic trends/patterns. Based on these patterns we drew out the five major thematic findings from the data. This accepted practice of thematically analyzing qualitative data helped us to gain a better understanding of end-user experiences and compare them with the responses from the other stakeholder groups to find similarities, differences, and gaps. This will also form the foundation of our future more in-depth research plans about the NID policy which is also evolving.

The draft version of this report was presented to a group of peer reviewers including academic researchers, journalists, digital and social justice advocates, and in-house colleagues. We presented the study to this group and then divided them into smaller groups; each smaller group examined the report from the perspective of one of the major findings. They reconvened and debriefed us with their observations and suggestions. Some of the recommendations have been included in this report. Other insightful observations were beyond the scope of this study which we have included in the conclusion as areas for future research. The peer consultation was a valuable exercise to include as part of the methodology to gain external perspectives on the report and make necessary edits and additions.

## *Conducting qualitative research during a pandemic*

### Opportunities, Challenges, and Ethical Considerations

As mentioned earlier, our initial research design was to conduct the qualitative study through the use of face-to-face interviews. Like many researchers around the world, we had to modify this method of collecting primary data considering the second wave of the COVID-19 pandemic which hit South Asia particularly hard during the summer of 2021. Countries once again went into national and/or regional lockdowns, travel was

[47] (Jacob & Furgerson, 2012)

restricted, and social distancing norms were reinforced.

The first wave of the pandemic had introduced the world to the benefits of using virtual meeting platforms such as Zoom, Skype, and Teams along with the video capabilities of instant messaging apps of WhatsApp and Signal to substitute the modalities of face-to-face interviews and focus groups. However, we faced challenges of low bandwidth and internet connectivity, especially in semi-urban and rural areas. We also faced the same internet problems in the capital of Kathmandu itself and could not use the video feature of Zoom when the researchers had to meet virtually. In the end, we found that using basic telephones and mobile phones was the only option available to us. While we acknowledge the benefit of being able to switch to telephonic interviews we also recognize the disadvantage of not being able to do face-to-face interviews which yield rich, non-verbal body language cues for qualitative researchers.

We also had to consider if conducting this study during the pandemic was too stressful for us and most importantly our respondents who were facing existential difficulties in health and livelihoods brought on by the pandemic. Here, our local interlocutors were very helpful and they were able to locally meet with respondents to figure out their willingness and ability to participate in the study. Another unplanned advantage of using local interlocutors was that they were able to identify six respondents who were not able to register for the NID card because of miscommunication with local coordinators.

We are thankful that despite delays we were able to complete this pilot study which will be the basis for future research about how the NID card impacts citizens in Nepal.

# Appendix B: Sample Populations

Total of 43 interviews

## Jhapa District - 18 interviews

### End-Users Jhapa

Total: 15
Gender distribution: Man 7; Woman 8
Persons with disability: Man 1 ; Woman 1
Geography: Urban 4 ; Rural  11

| Age group | Gender | |
|---|---|---|
| | Man | Woman |
| 20s | 3 | 4 |
| 30s | N/A | 2 |
| 40s | 1 | 1 |
| 50s | 2 | 1 |
| 60s | 1 | N/A |
| Total | 7 | 8 |

| Caste | Gender | |
|---|---|---|
| | Man | Woman |
| Brahmin | 4 | 3 |
| Janajati | 1 | N/A |
| Tharu | N/A | 2 |
| Dalit | N/A | 2 |
| Madhesi | N/A | 1 |
| Muslim | 1 | N/A |
| Unidentified | 1 | N/A |
| Total | 7 | 8 |

### Local Government Officials Jhapa

Total: 3
All 3 interviewees in their 50s
1 man, Janajati
2 women, both Brahmin

## Panchthar District - 19 interviews

### End-Users Panchthar

Total: 16
Gender distribution: Man 6; Woman 10
Persons with disabilities: 1
Geography: Semi-urban 5; Rural 11

| Age | Gender | |
|---|---|---|
| | Man: | Woman: |
| 20s | 1 | N/A |
| 30s | 2 | 5 |
| 40s | 1 | 2 |
| 50s | 1 | 3 |
| 60s | 1 | N/A |
| Total | 6 | 10 |

| Caste | Gender | |
|---|---|---|
| | Man: | Woman: |
| Brahmin | 2 | 1 |
| Janajati | 2 | 7 |
| Chhetri | 1 | N/A |
| Dalit | 1 | 2 |
| Total | 6 | 10 |

### Government Officials Panchthar

Total: 3
All 3 were men,
2 in their 30s and 1 in their 50s
Caste distribution: 2 Brahmin, 1 Chhetri

## Kathmandu District - 6 interviews

### Government Official Kathmandu

1 interviewee; interviewee details: Man, Brahmin, Urban

### Private Sector Kathmandu

Total: 3
All 3 were men, based in urban center
Caste distribution: 1 Newar (Janajati subgroup), 1 Other Janajati, 1 Chhetri

### Multilaterals Kathmandu

Total: 2
Both were Brahmin
1 man and 1 woman

# Appendix C

## *Recommendations for action*

### Update Digital Vocabulary and Terminology (for both Researchers and Policymakers)

The digital space is a volatile one where products, terms, and concepts are always in change mode. CSOs, policymakers, and the judiciary (to ensure that the laws keep up with the times) need to stay abreast of these changes and need to keep updating our digital vocabulary. Similar to any language that evolves over time and within the context of its usage, staying up-to-date with digital vocabulary is both a need and a responsibility for all of us who are engaged in this field.

### Recommendations for researchers and civil society organizations

#### *Follow up with an in-depth, mixed-methods study*

Our future research plans aim to conduct a larger mixed-methods study using both qualitative and quantitative methods including survey data from a larger sample population covering more districts and a weighted sample of marginalized groups that often get omitted from general population survey studies. The quantitative data will complement the granular and contextual information that we will continue to get from more interviews especially from marginalized population groups. We believe that using a mixed-method study as follow-up research will help us to understand and examine the NID card more closely. This will also enable us to offer holistic suggestions to policymakers about the largest stakeholder group — the end-users, whose lived experiences have not yet been taken into consideration.

#### *Collaborate with other civil society organizations working on digital rights*

Civil society organizations have as much responsibility as the press in democracies to hold public and private sector organizations accountable and responsible for public policies, such as the NID card which will impact the lives of all Nepalis in myriad ways.

Our secondary research examining global digital ID programs confirmed that organized and collaborative civil society scrutiny and action are growing in the digital rights space. The biggest and most powerful tech companies are incorporating civil integrity elements into their products and innovations. Simultaneously, multilateral agencies and governments are beginning to appreciate the value of having CSOs at digital policymaking tables to inform them from design to implementation to assessments.[48]

By working together across the spectrum of digital policy issues that impact the lives of our citizens, Nepal's digital rights CSOs must form a collective and organized voice to bring these perspectives to the forefront of policymaking forums.

### *Collaborate with other CSOs working at the intersection of social justice and digital policies*

Digital rights CSOs and CSOs working on other social justice issues such as public health, education, water and sanitation, food security, etc. must build networks of collaboration and the sharing of information. Digital policies such as the NID card when they are linked to other social services such as food rations, maternal health, schools, etc. impact the work of CSOs when working in these areas. When we begin to share information and collaborate across our practitioner silos we can gather richer data about how such policies impact communities as a whole across a range of issues rather than just the individual and their legal identity.

### *Engage with government and private sector actors to inform about grassroots challenges*

CSO engagements with both the state and private sector organizations have often been narrated through the lenses of confrontation and competition. CSOs have often been placed as opposing ends of the spectrum concerning policies, products, and advancing particular narratives of economic growth, development, and efficiencies of doing business. However, the fourth industrial revolution of digital transformation requires a more calibrated and collaborative approach to how these engagements are approached.

Civil society organizations appreciate the democratization and efficiencies that have occurred since the commercial use of the Internet but they also have immense experience working at the grassroots levels where these emancipatory technologies have either left behind, profiled, or disproportionately harmed vulnerable populations. The opportunity for the state and private sector companies to authentically engage with civil society organizations cannot be overstated. CSOs as representing the will of the public can keep the former two stakeholders fair, transparent, and accountable; they also help to create more inclusive and innovative products and services.[49] Development scholars and practitioners have witnessed that welfare programs that use a participatory model of active involvement of civil society and end-users in the design

[48] (Aggarwal, 2018); (Buzasu, 2020); (Digital IDs Rooted in Justice: Lived Experiences and Civil Society Advocacy towards Better Systems, 2022); (A Guide to Civil Society Organizations Working on Democratic Governance., 2005)

[49] (Buzasu, 2020); (The Future Role of Civil Society, 2013); (Civil Society in the Fourth Industrial Revolution: Preparation and Response, 2019)

and implementation stages have much higher rates of success.

It is our sincere hope that the Nepal government and Nepali companies will engage with us through this report and other policymaking forums where we can bring our experience and expertise to bear.

## Recommendations for policymakers

### *Adopt fair, accountable, and transparent digital policymaking and governance processes*

Policymakers should ensure that the spirit of multistakeholderism is embraced at every stage of the policymaking life cycle — from design to governance. This would make public policies fair and inclusive when all stakeholder views and experiences are taken into consideration. Our experience of working on the ground across a wide spectrum of development policy issues makes CSOs a good choice to have when designing and implementing digital ID policies, since they intersect with practically all areas of a citizen's life.

Regular assessments including risks and challenges faced by all stakeholder groups when engaging with digital policies should become the norm so that they can be reviewed and modified appropriately. Such assessments and resulting policy changes should also be reflected in their governance and be easily accessible in the public domain. This would make these large-scale digital policies accountable to the public they purport to serve.

Finally, all policies should be transparent in terms of clear and complete dissemination of policy procedures: from registration to data collection, storage, usage of the databases, and all governance processes, including the other uses for which data is being collected beyond legal identification for social service delivery as well as identifying which authorized agencies (public and private) the databases will be shared with.

A strategic communication policy, using a diverse range of communication channels to reach all citizens, should be a part of this transparency plan. Effective communication regards transparency of procedures will reduce misinformation and misuse of the policy, and will increase faith and credibility in government departments entrusted with implementing these policies.

### *Protect data and digital privacy of citizens*

In light of the government's overarching Digital Nepal Framework and the multi-purpose NID card wherein large swathes of personal sensitive data is being collected, the government must reassess the existing Privacy Act 2018 and Guidelines 2020. The government must include the active consultation of all stakeholders to discuss if we need separate data protection legislation that addresses the specific issues of a digital era with massive digital policies such as the NID card, that can impact all areas of a citizen's life. National security, national sovereignty, public authorities, law enforcement, public good, and research purposes are terms used in the existing Privacy Act that are not well defined, ambiguous, and provide too many exceptions to the concept of informed consent and privacy of personal data. These need to be carefully scrutinized to ensure that neither the state nor non-state actors can misuse citizens' sensitive demographic and biometric data.

This would act as a legal safeguard against any misuse of data and enact adequate regulations for the collection of data that meets internationally accepted standards of proportionality and minimization. Citizens are being made to provide their demographic and biometric data to gain access to public and private goods and services, with an ambiguous legal recourse for them when their data is breached or misused.

### *Ensure robust cybersecurity standards and protocols*

Rapid digitization has also increased the threat of cybersecurity vulnerabilities and data breaches even in the most technologically advanced countries. Policymakers must ensure that the highest and most robust cybersecurity standards and encryption of databases are used to protect citizens' data. Global South countries tend to adopt lower standards of encryption to enable greater access to digital communications.

Further, cybersecurity protocols being used must follow principles of transparency as well so that ethical hackers and the cybersecurity research community can regularly test them for bugs and vulnerabilities. Bug bounty programs are highly effective and used by the largest tech companies and government departments around the world to detect digital vulnerabilities and fix them.

### *Reevaluate the use of technological solutions*

Our past research and this pilot study have repeatedly revealed that technological solutions to socio-culturally rooted structural inequities lead to further marginalization. For example, a patriarchal social system in Nepal has led to women having unequal access to education, opportunities for work, and financial independence. This results in their limited access to smartphones and online resources to leverage the benefits that tech solutions promise; these are available to men and other privileged groups more easily. We therefore urge policymakers to reevaluate existing social structural barriers and find culturally contextual initiatives to eradicate these before presuming that tech solutions will be a panacea to all social problems.

This study and other evidence across the world reveal exclusion from the digital ID card system could mean one not being able to access public and/or private services. Such exclusions will only increase existing social disparities and make the system more exclusionary. Policymakers need to ensure even those who are unable to access NID for any reason should still be able to access available services.

### *Create a national digital literacy mission*

This study reconfirmed our earlier findings that digital literacy and awareness are low among the general population, who have adopted tech such as social media platforms and e-commerce without sufficient knowledge about the basics of data protection, digital privacy, online harms, and cybersecurity threats. We think it is vital for policymakers to consider launching a responsible, ethical, and current digital literacy mission that prepares Nepali citizens for the double-edged sword of a digital era. One where they can leverage the promises of a transformative digital future with full knowledge of how to protect themselves from the vulnerabilities and threats of this space.

# Bibliography

*A Guide to Civil Society Organizations Working on Democratic Governance.* (2005). UNDP. http://www.undp.org/content/dam/aplaws/publication/en/publications/democratic-governance/oslo-governance-center/civic-engagement/a-guide-to-civil-society-organizations-working-on-democratic-governance-/3665%20Booklet_heleWEB_.pdf

*Aadhaar Dashboard*. (2019, October). UIDAI. https://uidai.gov.in/aadhaar_dashboard/

Abraham, R., & Pattanayak, A. (2018, January 16). Clearing the air on Aadhaar data breach. *Mint*. https://www.livemint.com/Opinion/MUPJK28VMeoICzl1whSBrJ/Clearing-the-air-on-Aadhaar-data-breach.html

Aggarwal, R. J. S. C., Wafa Ben-Hassine, Naman M. (2018, March 22). National digital identity programmes: What's next? *Access Now*. https://www.accessnow.org/national-digital-identity-programmes-whats-next/

Alessandro, A. (2019, July). *Does Privacy Actually Matter? - News - Carnegie Mellon University*. http://www.cmu.edu/news/stories/archives/2019/july/world-economic-forum-acquisti.html

Anamitra, D., Ranasinghe, E., & Saltuk, Y. (2017). *Trust and Privacy* [Blog]. Omidyar Network. https://medium.com/omidyar-network/trust-and-privacy-cb27e85fecf5

Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good* (1st ed., pp. 44–75). Cambridge University Press. https://doi.org/10.1017/CBO9781107590205.004

Baxter, P., & Jack, S. (2015). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*, 544–559. https://doi.org/10.46743/2160-3715/2008.1573

Bennett, C. J. (Ed.). (2012). *Privacy advocates, privacy advocacy and the surveillance society in Routledge handbook of surveillance studies*. Routledge: Taylor & Francis Group.

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies*, *13*(1), 5–24. https://doi.org/10.1177/1367877909348536

Bhadra, S. (2019, June 18). Five Surprisingly Consequential Decisions Governments Make About Digital Identity. *Omidyar Network*. https://omidyar.com/five-surprisingly-consequential-decisions-governments-make-about-digital-identity/

Buzasu, C. (2020, June 19). *The role of civil society in policymaking*. Apolitical. https://apolitical.co/solution-articles/en/the-role-of-civil-society-in-policymaking

Chakravorti, B. (2018, July 23). *As emerging economies bring their citizens online, global trust in internet media is changing*. The Conversation. http://theconversation.com/as-emerging-economies-bring-their-citizens-online-global-trust-in-internet-media-is-changing-95262

Chautari, M. (2022, February 1). "नेपालको सन्दर्भमा राष्ट्रिय परिचयपत्रका विभिन्न आयाम [Social Media

Post]. Facebook.

*CIGI-IPSOS Global Survey on Internet Security and Trust*. (2014). CIGI-Ipsos.

*Civil Society in the Fourth Industrial Revolution: Preparation and Response*. (2019). World Economic Forum.

Country case-study: Sexual and reproductive rights in India. (2020, June 8). *Privacy International*. http://privacyinternational.org/long-read/3863/country-case-study-sexual-and-reproductive-rights-india

*Cyber Security in the Global South*. (2017). Privacy International. https://privacyinternational.org/sites/default/files/2017-12/Cybersecurity_2017.pdf

*Digital IDs Rooted in Justice: Lived Experiences and Civil Society Advocacy towards Better Systems*. (2022). The Engine Room. https://www.theengineroom.org/wp-content/uploads/2022/01/Engine-Room-Digital-ID-2022.pdf

*Digital India: Unleashing Prosperity*. (2015). Deloitte Touche Tohmatsu India Private Limited. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-tele-tech-2015-noexp.pdf

Dixon, P. (2017). A Failure to “Do No Harm”—India’s Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. *Health and Technology, 7*(4), 539–567. https://doi.org/10.1007/s12553-017-0202-6

*Dr. Usha Ramanathan declared “Hero” for speaking out against India’s controversial Aadhaar digital identity program*. (n.d.). Access Now. https://www.accessnow.org/press-release/usha-ramanathan-human-rights-hero/

*“Everyone said no” Biometrics, HIV and Human Rights A Kenya Case Study*. (2018). KELIN and the Kenya Key Populations Consortium.

Fluri, J. L., Jackson, P. S. B., & Paudel, D. (2015). A New Development Technology? South Asian Biometrics and the Promise of State Security and Economic Opportunity: A New Development Technology? *Geography Compass*, *9*(10), 539–549. https://doi.org/10.1111/gec3.12230

Frowd, P. (2010). Identifying Citizens: ID Cards as Surveillance. *Canadian Journal of Sociology, 35*(1), 205–207. https://doi.org/10.29173/cjs7462

Handa, R. (2016, March 9). *Multistakeholderism in cybersecurity: What civil society brings uniquely*. Internet Democracy Project. https://internetdemocracy.in/2016/03/multistakeholderism-in-cybersecurity-civil-society

*ID2020 Summit 2016 | United Nations Office for Partnerships*. (n.d.). UN Office for Partnerships. https://unpartnerships.un.org/news/id2020-summit-2016

Jacob, S., & Furgerson, S. (2012). Writing Interview Protocols and Conducting Interviews: Tips for Students New to the Field of Qualitative Research. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2012.1718

Justice K.S. Puttaswamy (Retd.) & Anr. Vs. Union of India & Ors., (Supreme Court of India

2017).

Kayastha, S., & Mamata, P. (2020). *Identities experiencing the internet: Nepal Survey Report*. Body & Data.

Khan, M., & Roy, P. (2019). *Digital identities: A political settlements analysis of asymmetric power and information*. SOAS University of London. https://ace.soas.ac.uk/publication/digital-identities-a-political-settlements-analysis-of-asymmetric-power-and-information/

Khera, R. (2017). *Impact of Aadhaar in Welfare Programmes* (SSRN Scholarly Paper No. 3045235). https://doi.org/10.2139/ssrn.3045235

Khera, R. (2018). The Aadhaar debate: Where are the sociologists? *Contributions to Indian Sociology*, *52*(3), 336–342. https://doi.org/10.1177/0069966718787029

Khera, R. (Ed.). (2019). *Dissent on Aadhaar: Big data meets big brother*. Orient BlackSwan.

Leurs, K., & Shepherd, T. (2017). *Datafication & Discrimination*. https://doi.org/10.25969/MEDIAREP/12456

Lisko, T. (2014, November 20). *Cybersecurity as Realpolitik by Dan Geer*. PrivacyWonk. https://www.privacywonk.net/2014/11/cybersecurity-as-realpolitik-by-dan-geer/

Lohr, S. (2018, February 9). Facial Recognition Is Accurate, if You're a White Guy. *The New York Times*. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

Man Maharajan, H. (2021, March 6). Privacy, Security Issues Of National ID Card. *Martin Chautari*. http://www.martinchautari.org.np/blogs/1059

Manzar, O. (2017, September 21). *Privacy and the Indian culture*. Mint. https://www.livemint.com/Opinion/rM3vgXErD5oWiv12IEaKcK/Privacy-and-the-Indian-culture.html

Mathews, L. (2021, January 30). Hackers Breach U.S. Cellular Customer Database After Scamming Employees. *Forbes*.

*National IDs Around the World—Interactive map*. (n.d.). World Privacy Forum. https://www.worldprivacyforum.org/2021/10/national-ids-and-biometrics/

Paraskevopoulos, D. (2021, August 18). Estonian e-state has experienced several hacking incidents as of late: What are the lessons learned? *E-Estonia*. https://e-estonia.com/estonian-e-state-has-experienced-several-hacking-incidents-as-of-late-what-are-the-lessons-learned/

Robinson v. Attorney General, (Supreme Court of Judicature of Jamaica April 12, 2019).

Sharma, A. (2016, September 9). World Bank approaches Unique Identification Authority of India to share its experiences with other countries. *The Economic Times*. https://economictimes.indiatimes.com/news/politics-and-nation/world-bank-approaches-unique-identification-authority-of-india-to-share-its-experiences-with-other-countries/articleshow/54204185.cms

Sharma, B. (2022, January 11). People queue up overnight for e-passport, national ID card. *My Republica*. https://myrepublica.nagariknetwork.com/news/people-queue-up-overnight-for-e-passport-national-id-card/

Sinha, A., & Kodali, S. (2017). *Information Security Practices of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar Numbers with sensitive personal financial information*. Centre for Internet & Society. https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1

Success Story – Estonia's 20 years of Digital Transformation – The Digital Republic. (2020, October 9). *Risalat Consultants International*. https://risalatconsultants.com/success-story-estonia-20-years-digital-transformation/

Suite 800. (2017). Few worldwide have a lot of trust in their government. *Pew Research Center*. https://www.pewresearch.org/global/2017/10/16/many-unhappy-with-current-political-system/pg_2017-10-16_global-democracy_1-03/

Sur, A. (2021, October 18). Landmark Ruling Finds Kenya's Government Illegally Rolled Out Aadhaar-Like Biometric ID. *MediaNama*. https://www.medianama.com/2021/10/223-kenya-high-court-huduma-numba-illegal/

The Constitution of Nepal 2015. Article 51, Section (3). https://www.mohp.gov.np/downloads/Constitution%20of%20Nepal%202072_full_english.pdf

*The Future Role of Civil Society*. (2013). World Economic Forum.

*Trust in government: 1958-2015*. (2015, November 23). Pew Research Center. https://www.pewresearch.org/politics/2015/11/23/1-trust-in-government-1958-2015/

White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M., & Sperling, O. (2019). *Digital identification: A key to inclusive growth*. McKinsey Digital. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

*World Bank ID4D*. (n.d.). https://id4d.worldbank.org/about-us

*World Development Report: Enabling Development—Digital IDs*. (2016). World Bank.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First edition). PublicAffairs.

# Digitization of Identity in Nepal: Efforts, Experiences and Effects

Body & Data

Body & Data is a digital rights organization in Nepal that aims to increase women and queer persons' engagement in digital spaces through suitable strategies for expression, autonomy and agency.

bodyanddata.org