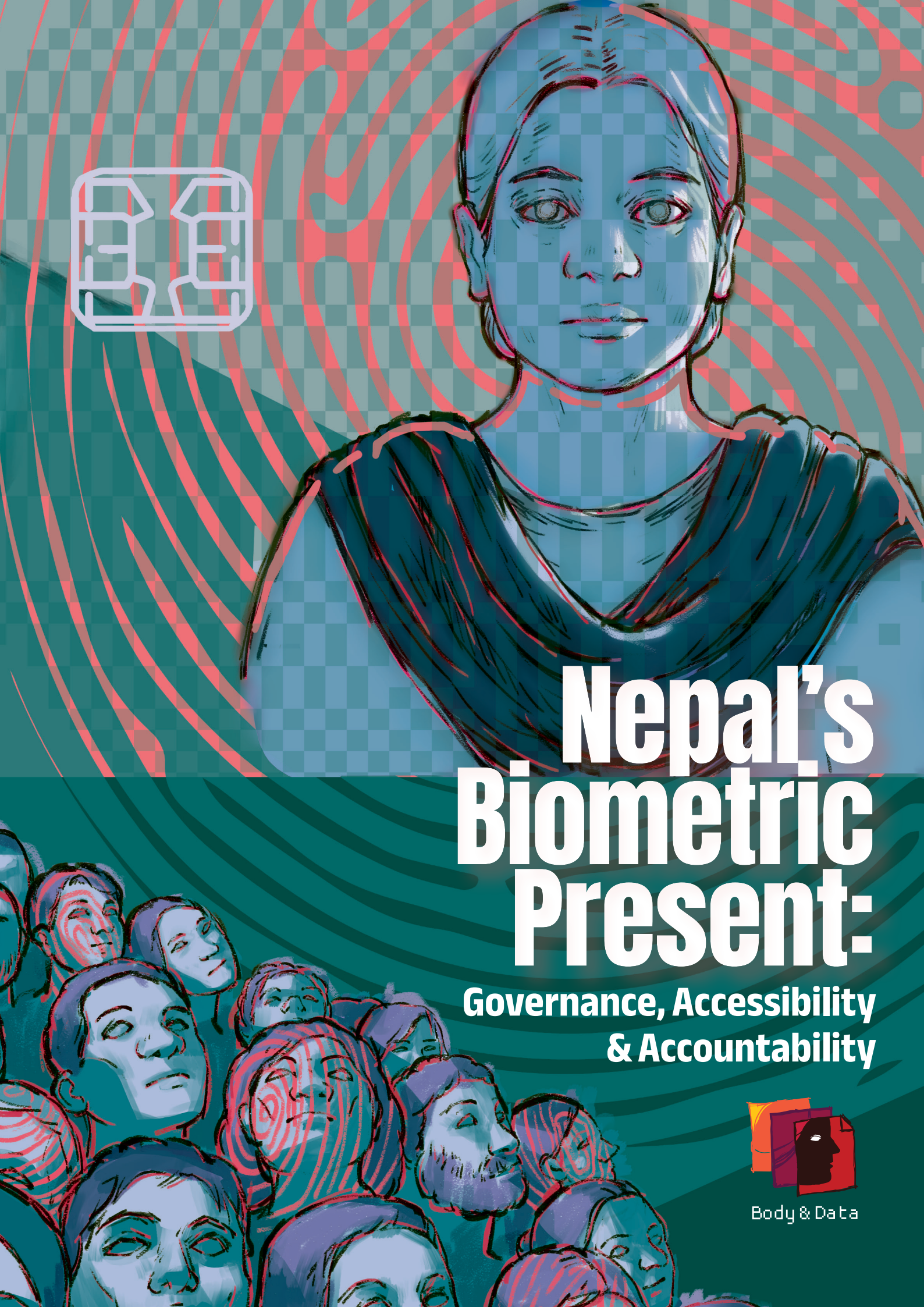


Nepal's Biometric Present:

Governance, Accessibility & Accountability

Body & Data

NEPAL'S BIOMETRIC PRESENT: ACCESS AND ACCOUNTABILITY

This report is based on the study conducted by Body & Data in the districts of Sarlahi, Khotang, 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 practitioners, 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 Contribution
Bhaskar Gautam, Dovan Rai, Rita Baramu, Shubha Kayastha
Sapana Sanjeevani, Monika, Nuva Rai

Research Assistants/Local Coordinators
Irshat Khatoon, Malangwa Municipality, Sarlahi District
Barsha Rai, Diktel Municipality, Khotang District

Copy-Editing
Shafali Uprety

Cover Illustration
Supriya Manandhar

Layout and Design
Sixwasnine Design

Financial Support
Open Society Foundation (OSF)

CONTENTS

ACRONYMS

BPL	Below Poverty Line
CBO	Civil Society Based Organization
CDO	Chief District Officer
CSO	Civil Society Organization
DAO	District Administration Office
DONIDCR	Department of National Identity and Civil Registration
DPI	Digital Public Infrastructure
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
ID	Identity Document
IDEEA	ID Enabling Environment Assessment
NID	National Identity Card
NIN	National Identity Number
NIDMIS	National Identity Management Information System
NGO	Non-governmental Organization
PIN	Personal Identification Number
PWD	People with Disabilities
SDG	Sustainable Development Goal
UIDAI	Unique Identification Authority of India
UIN	Unique ID/identity number
WPF	World Privacy Forum

TERMINOLOGIES USED

The terms used in this study have been selected based on the definitions outlined below. Our sources include global legislation such as the General Data Protection Regulation (GDPR), academia, industry leaders in cybersecurity, civil society organizations (CSOs), as well as consumers.

Aadhaar Card/Aadhaar Number:

It is a 12-digit unique number issued by the Unique Identification Authority of India (UIDAI) to residents of India upon completion of a prescribed verification process. Any resident, irrespective of age or gender, can voluntarily enroll to obtain an Aadhaar number. While it functions as proof of identity, it does not grant citizenship or domicile rights.

Biometric Data:

Personal data that captures an individual's physical, physiological, or behavioral characteristics through technological processing and is used to confirm their unique identity as biometric data. This can include, but is not limited to, voice recognition, fingerprint scanning, facial recognition, iris recognition, and heart-rate sensors. When such data is collected and utilized without strong legal protections, it opens the door to extra-judicial surveillance by state and private entities, posing serious risks to data privacy as individuals' bodies become quantifiable elements of their identity.

Cybersecurity:

The application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks, and to prevent unauthorized access or exploitation.

Data Breach:

A cybersecurity incident in which information is stolen or accessed from a system without the knowledge or authorization of its owner. It results in the exposure of confidential, sensitive, or protected data to unauthorized entities. The compromised files may be viewed, shared, or altered without permission. Data breaches can affect individuals, businesses, and governments, and anyone lacking proper safeguards can inadvertently endanger others.

Datafication:

The process of transforming various aspects of life, such as human activities, behaviors and interactions, into quantifiable data that can be stored, analyzed and used. This includes not only traditional data like names or addresses but also digital traces such as location history, social media activity, and biometric details such as facial features and fingerprints.

Demographic Data:

Socioeconomic information or variables include name, age, gender, address, marital status, religion, caste, ethnicity, race, employment status, and income level. These variables can be statistically expressed to represent different population groups.

Digital Literacy:

It builds on basic literacy skills to provide an understanding of how digital technology works and how to use it effectively. It includes skills such as evaluating online information, using digital devices, navigating the internet, and being aware of key issues such as privacy, cybersecurity, informed consent, and data breaches.

Digital Identity (Digital ID):

An online representation of an individual constructed from both explicit data we provide, such as account sign-ups, posts, and photos, and implicit data collected through our actions, like browsing history and purchase patterns.

Digitalization:

The process of using digitized information and digital technologies to transform public and private sector operations, services, and policies. It is often based on the assumption that digital systems offer greater efficiency, accuracy, and scalability than traditional manual processes.

Digitization:

The conversion of analog information, records, or objects into a digital form that can be processed by a computer and specialized devices.

Digital Public Infrastructure (DPI):

A set of foundational digital systems, mainly identification, payments, and data sharing, that serve as building blocks for delivering digital services. They also serve as an intermediate layer in the digital ecosystem.

Digital Privacy:

The principle that individuals should control how their digital information is collected, used and shared. It also refers to the ability to safeguard digital information from unauthorized access, misuse, or exposure, ensuring that it remains secure, confidential, and within the individual's control.

E-Passport (Electronic or Biometric Passport):

An international travel document that includes identity information such as passport number, name, nationality, and date of birth, along with a microprocessor chip containing biometric data like fingerprints, photos, and signatures. These passports are scanned using specialized devices.

Information Security:

The tools, practices and processes used to safeguard sensitive digital information from unauthorized access, alteration, destruction, or disruption. It ensures the confidentiality, integrity, and availability of data.

Personal Data:

Any information related to an identifiable individual, including names, identification numbers, location data, online identifiers, and characteristics such as physiological, genetic, mental, economic, cultural, or social identity.

Profiling:

Any automated processing of personal data to evaluate or predict aspects of an individual's life, including job performance, economic status, health, preferences, interests, reliability, behavior, and location.

Sensitive Data:

This category of personal data includes sensitive information such as racial or ethnic background, political opinions, religious or philosophical beliefs, trade union membership, genetic, and biometric details (especially when used for identification purposes). Due to its nature, this type of data demands enhanced protection and strict security measures.

Social Exclusion:

It is a complex and multi-dimensional process marked by the denial of access to essential resources, rights, services and opportunities. It also entails exclusion from full participation in social, economic, cultural, and political life enjoyed by the majority. Social exclusion negatively impacts individual well-being and undermines social equity and cohesion.

Unique Identification Number (UIN):

A unique number assigned to an individual that serves to identify them and connect their identity across various public and private databases. National identity authorities may issue this UIN to residents or citizens for use throughout their lifetime.

EXECUTIVE SUMMARY

In November 2018, the Government of Nepal introduced the 'National ID' (NID) to provide digital identity to its citizens. The government ambitiously claimed to enroll all residents biometrically by 2023. Each enrolled person would receive a unique 10-digit identification number, which would serve as their National ID. This number would be linked to their biometric data, such as a digital photograph, fingerprints, and iris scans, as well as personal details like name, address, and gender. The NID is an identification process designed for easy online identity verification, but its digital use has been very limited since it started in 2018.

This study examines the social consequences and on-the-ground effects of the National ID. It explores three key aspects: public understanding of the National ID, the political ambitions of the Nepali state associated with biometric projects, and users' experiences while enrolling for the Digital ID. The scope of this study is confined to answering three questions:

WHY IS THE NEPALI STATE PURSUING DIGITAL IDENTIFICATION?

HOW IS THE GOVERNMENT EXECUTING ITS DIGITAL IDENTIFICATION SCHEME?

HOW ARE CITIZENS ENGAGING WITH THE GOVERNMENT'S AMBITIOUS BIOMETRIC INITIATIVE?

As NID cards are not yet widely used in digital form, mainly because public offices and stations lack card-reading machines, this study presents an overview of the project's design, planning, and implementation, with a focus on the enrollment process. It builds on Body & Data's earlier research conducted during the pilot phase of the identification project.

By late 2024, over 16 million citizens had been mandatorily enrolled in the National ID system. The distribution of ID cards, which began in 2022, has recently gained momentum, with more than 1.5 million cards issued. While the NID serves as a tool of digital identification, it is not proof of citizenship and it does not confer citizenship rights. However, access to the NID is currently limited to residents who possess citizenship certificates. As a result, millions of residents – particularly the landless, marginalized groups, and children of single mothers who lack such documentation – are excluded from the digital system.

The Nepal government expects the NID to promote efficient governance through the use of "digital solutions" by ensuring interoperability and improved access to services. The NID is intended to serve as personal identification and to interoperate across both public and private sectors as a digital ID. At this stage, NID is not used for delivering welfare benefits. The program aims to standardize the fragmented system of existing documents such as citizenship certificates, driving licenses, election IDs, Below Poverty Line (BPL) cards, into a singular ID.

The study found many gaps in the ambitions and promises made by the government and its implementation and delivery. Nepal's policy guidelines on the NID appear

to follow a top-down approach, with limited understanding and inadequate public consultations. The government is advancing its vision of "smart" governance without making adequate investments in digital public infrastructure (DPI). Limited investment in digital foundations, technology adoption, data protection frameworks, and efforts to bridge the digital divide have led to a weak DPI and poor public understanding.

The administrative workforce was not systematically reoriented to support digital transformation, leading to the continuation of traditional implementation practices. This has been further exacerbated by inadequate education, training, and awareness programs regarding information and communications technology (ICT) and biometric systems. Overall, the implementation has lacked proactive public engagements and educational efforts, particularly concerning digital literacy, privacy and data protection issues.

Citizens have emphasized that mandatory enrollment in the National ID system is simply an additional burden, requiring them to obtain yet another form of ID. While the government plans to link NID with social security allowances, there is currently no guarantee of additional welfare services. For citizens, this results in bureaucratic burden. For the government, identifying citizens without providing meaningful services suggests a greater focus on surveillance and public security rather than on social security and inclusion.

During the enrollment process, the federal government engaged in limited intergovernmental consultation and coordination. The role of District Administration Offices has been reduced to basic implementation, with municipalities facilitating implementation on the ground. It was reported that local authorities only received brief orientation sessions focused on how to operate enrollment stations and collect citizens' data. Consequently, local government officials themselves lacked clarity about the potential digital uses of the NID. This lack of information significantly impacted end-users, who were not adequately informed about its use, as well as about privacy and biometric data protection.

The NID card has been integrated into existing bureaucratic procedures, but the transition toward "smart" governance has lacked systematic planning and strategic direction. This, along with a traditional administrative mindset, has hindered the enrollment process, which continues to face challenges such as weak digital infrastructure, poor connectivity, uneven internet access, and frequent power outages. These issues have affected citizens, especially women, the poor, and marginalized groups. Although existing policies acknowledge the physical barriers faced by persons with disabilities, in practice, they continue to encounter discriminatory administrative practices.

Civil Society Organizations (CSOs), including those in the private sector, are still relatively new to digital literacy and digital rights, making them less informed about the National ID and its biometric implications. They were not consulted during the planning and implementation phases of the project. Meaningful public consultation and cross-sectoral dialogues on biometric data were notably absent. This highlights the essential role digital rights organizations can play in ensuring accountability from governments and multilateral agencies. It also reveals the largely rhetorical nature of current narratives surrounding digital solutions for improved governance and inclusivity.

I. INTRODUCTION

Nepal's new digital identification system is considered a "*game changer*" within state institutions, especially by government authorities.[1] Launched in November 2018, this system is called the "*National ID*" with the main purpose of digitizing the identification of Nepali citizens. The digitization programs reflect universal claims that the absence of a universal identity creates conditions of insecurity and exclusion. Nepal's Digital ID framework, with an emphasis on security and inclusion has been modelled on the World Bank's D4D document.[2]

Although the National ID process was initiated earlier, the National ID and Civil Registration Act came into effect in August 2019. As outlined in its Preamble, the Act mandates that all citizens must obtain a National ID. However, under Article 4, only Nepali residents possessing a citizenship certificate are eligible to acquire the NID.[3] This provision automatically excludes millions of people who lack citizenship certificates, typically issued at age 16 or later.

Citizenship certificates are a prerequisite for accessing a wide range of services and rights, including birth or marriage registration, higher education or professional examinations, civil service positions, employment, voting rights, land and property ownership; social welfare benefits, and financial services.[4] Historically, marginalized groups – such as individuals affected by caste or ethnic discrimination, children of single mothers, those living in poverty, or internally displaced persons – have often been denied citizenship certificates and, consequently, are also excluded from obtaining the National ID.

Following the Nepal Citizenship Act, 2006, citizens who were granted citizenship certificates based on birth right, and their children, approximately 1.2 million in number, were excluded from accessing citizenship certificates. Consequently, they were unable to enroll digitally until recently. In June 2023, the Supreme Court cleared the way for the Nepal Citizenship First Amendment Act, which had been delayed for years. With the amendments, these individuals now have access to citizenship certificates and subsequently to a NID.

On the issue of citizenship through either the mother or father, despite fundamental rights being coded in the Interim Constitution of Nepal, Section 8(1)(a) of the Nepal Citizenship Act of 2006 contradicted the constitutional provision of Article 11(2) by imposing restrictions on children of Nepali women married to foreign nationals. Women's rights advocates demanded the removal of this provision from the Act, as it is discriminatory to women and their children who are unable to obtain citizenship certificates or enroll digitally. In order to ensure the dignity of both the mother and the child, the Interim Constitution also introduced a new provision guaranteeing the rights of a single mother. However, in practice, providing a written statement from the mother or the applicant stating that the father is either unidentified or untraceable was not considered sufficient to obtain citizenship certificates in the name of the mother, thus denying access to citizenship rights and subsequent digital enrollment. Although Nepal's new constitution in 2015 and a court ruling in 2017 allowed mothers to pass on citizenship to their children, in practice obtaining citizenship certificates has not been easy due

to gender discrimination. For example, although an individual can obtain a citizenship certificate that aligns with their gender and sexual orientation, members of the LGBTQI+ community face several barriers and discrimination in practice.

With the launch of the NID, the government ambitiously claimed that by 2023, all Nepali residents would be biometrically enrolled. Each resident would receive a unique 10-digit identification number, serving as their "National Identity" number, connected to a record containing their personal biometric data and a set of social data. Biometric data capture a digital photograph, fingerprints, and an iris-scan record, while social data includes name, address, and gender. The NID is designed for online identity verification across government and private platforms, theoretically allowing citizens to access online services easily.

Nepal's capacity to advance its digital identification measures will be tested in the coming years, contingent upon the effective implementation and adaptation of the National ID system. This "internationally celebrated" system is projected to deliver cost-efficient and secure means of identification,[5] with a particular emphasis on enhancing "interoperability" across diverse sectors, including security operations, welfare projects, and commercial services.[6]

As in other countries, Nepal's investment in a digital identification system aims to enhance accountability in public security and improve citizens' access to social services while upholding their rights. The government emphasizes on its official website that biometric technology has become a trusted "digital solution" for "smart" governance,[7] shaping new security spaces.[8] Automated surveillance is provided to ensure public security, preventing "unwanted entrants" through facial recognition, biometric verification, and authentication of demographic information when necessary.[9] The goal is to maintain peaceful order and improve the efficiency of public services, by digitizing citizen identification.

This study found that, despite claims of gains in digital governance, there are tradeoffs, as the digital shift introduces new forms of surveillance, exploitation, and exclusions.[10] It was also found that, amidst existing digital divides and lack of digital literacy, rights-based organizations and informed citizens are working to critically engage with proposed digital solutions and their discriminatory measures.

There is a growing interest in improving social services and protecting citizens' rights, especially among major development organizations like the World Bank and the United Nations. One clear example of this is the Sustainable Development Goals (SDGs). In particular, SDG 16.9 highlights the importance of providing everyone with a legal identity, including birth registration. According to this goal, legal identity is a basic requirement for building peaceful, fair, and inclusive societies. It also helps people gain access to justice, participate in elections, receive social benefits, use banking services, and find jobs more easily.[11]

To meet these goals, many development programs are implementing new types of digital identification systems. These digital IDs are seen as a more efficient and cost-effective way to ensure that people are included in important services. As a result,

both international donors and local civil society organizations, including NGOs and community-based groups, are supporting these efforts.

However, in trying to make identification more modern and efficient, some governments and donors are working with private companies in a way that may separate identification from actual citizenship rights. They justify this by saying it will make access to services more secure and inclusive. But this shift raises concerns about whether people's full rights as citizens are still being respected in the process.[12]

For citizens, issuing proof of their identity to access any service is not a new concept. Historically, citizens have used various documents issued by the state to confirm their identity, such as Citizenship Certificates, driving licenses, election identity cards, and Below Poverty Line (BPL) cards. The digitization program aimed at creating a NID card is intended to streamline this array of documents by providing a singular ID. This new identity card serves as a standardized form of personal identification accepted nationwide.

By introducing a standardized national identity for both public and private sectors, the government aims to achieve the objectives of preventing fraud, enhancing cost efficiency, and promoting transparency. However, citizens are questioning the necessity of the National ID, as expressed by a respondent from Khotang: "Why do we need a National ID when we already have a citizenship certificate? It seems unnecessary, especially since the government hardly offers subsidies or allowances based on it."[13]

About this study

This study examines the social consequences and real-world impacts of identification processes by exploring the concept of the National ID, the political goals of the Nepali state related to biometric projects, and the experiences of users with this digital technology. The focus of this study is narrowed down to three main questions:

a) Why is the Nepali state pursuing digital identification?

b) How is the government implementing its digital identification program?

c) How are citizens engaging with the government's ambitious biometric initiative?

This study expands on Body and Data's previous research on the National ID (see Box 1), which focused on the pilot phase of the identification project.

The study was carried out between September 2022 and November 2023 in three districts: Kathmandu, Sarlahi, and Khotang. An additional round of interviews was conducted in Kathmandu in November 2024. In Kathmandu, interviews and consultations were held with government officers, political representatives, policy practitioners, civil society actors, and rights based advocates.

Khotang and Sarlahi were selected based on the government's enrollment performance assessment – Khotang was categorized as a "successful" district, while Sarlahi was identified as "difficult". In both districts, data was

Box 1: Digitization of Identity in Nepal: Efforts, Experience and Effects

In 2021, Body & Data conducted a pilot study titled Digitization of Identity in Nepal: Efforts, Experiences, and Effects, which explored stakeholder perspectives during the inception phase of the NID program.

The study focused on how end-users navigated the registration process, their lived experiences, and the broader impacts of the program on their daily lives.

The findings aligned with global critiques of digital ID systems, revealing significant gaps between policy promises and on-the-ground realities. While governments and multilateral institutions often promote digital IDs as tools for inclusive development and efficient service delivery, the study found that such claims tend to overstate benefits while downplaying harms, particularly for marginalized communities.

Key concerns identified in the study include:

- **LACK OF MULTISTAKEHOLDER ENGAGEMENT:** The NID program was launched without adequate public consultation or transparency, particularly with communities most affected by such policies.
- **CENTRALIZED DATA AND MULTIPURPOSE USE:** The use of a centralized database and the integration of NID with both public and private services increases the risk of misuse, data breaches, and lack of accountability.
- **INCREASED SURVEILLANCE RISKS:** Biometric data collection, such as fingerprints and iris scans, goes beyond identification, raising the potential for persistent surveillance and privacy violations.
- **SOCIAL EXCLUSION:** The system risks reinforcing or worsening existing inequalities, especially for women in patriarchal contexts, people with disabilities, migrants, and LGBTQI+ individuals.

Body & Data approached this study through a qualitative lens. Semi-structured interviews were conducted with end-users, government officials, data collection contractors, private actors, and multilateral agencies involved in the NID rollout.

These narratives were thematically analyzed alongside existing research, policy frameworks, and media reports to present a grounded, rights-based critique of the digitization of identity in Nepal.

collected through interviews with political representatives, government officials, professionals, civil society actors, and media practitioners. Focus Group Discussions (FGDs) were conducted with women, ethnic and religious minorities, economically disadvantaged and vulnerable populations. In Kathmandu, FGDs were also held with civil society organizations and specific interest groups such as People with Disabilities (PwD) and queer communities.

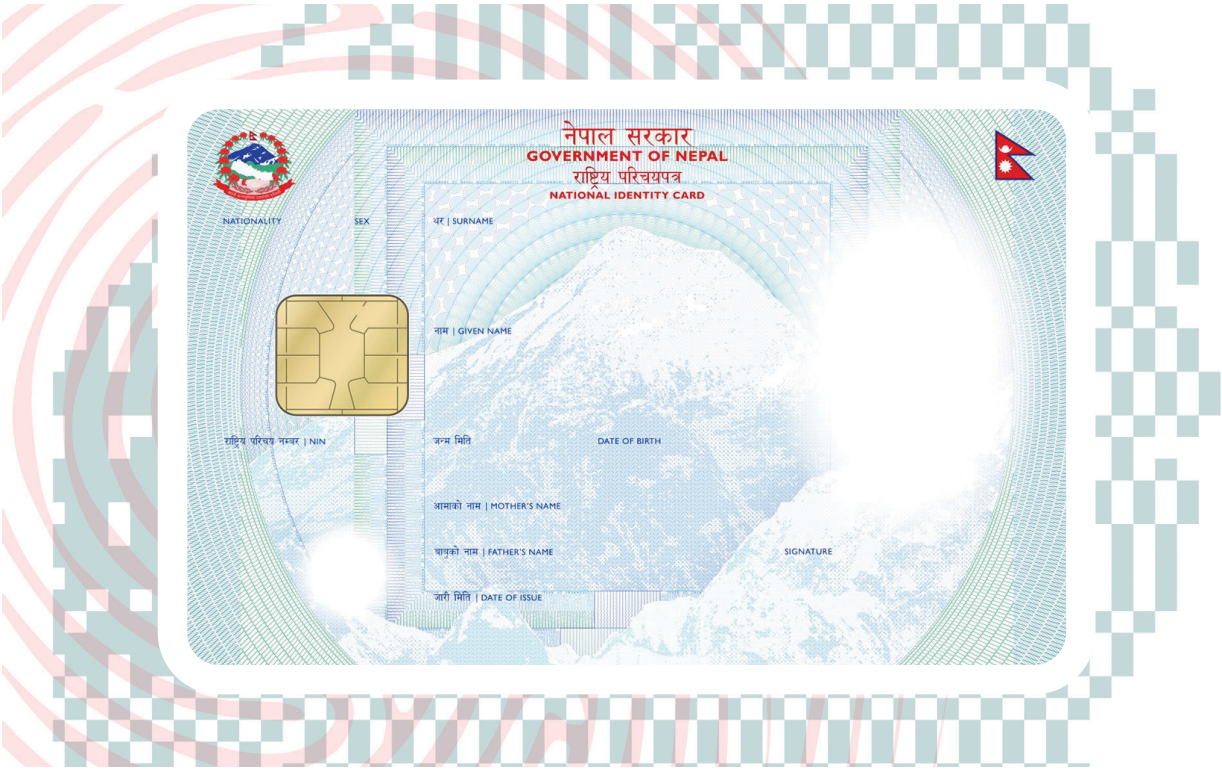
Drawing on primary government records, field based observations, in-depth interviews, consultative meetings, and FGDs, the qualitative study for this report was conducted by a six-member team with additional support from two research assistants, one in Sarlahi and one in Khotang. In total, 365 individuals were consulted, including 45 individual interviews and 318 group participants in nine FGDs. Seven consultative meetings were held with CSOs, media practitioners, private sector professionals and rights based advocates. Interviews were conducted with government authorities, former directors, senior officers, implementing officers, concerned staff, technical in-charge and actors involved in drafting digital bills.

During the field research conducted outside the Kathmandu Valley, data collection for the NID card was in progress. However, the distribution of the cards had not yet commenced. Nonetheless, by the end of 2024, the distribution process had been accelerated.

This report is organized into four sections: the origins of the National ID, its implementation, disputes and differences, and citizens' concerns for privacy. The first section on origin seeks to understand how policy priorities were conceived and plans were designed. The implementation section examines how the Nepali state's political ambition is unfolding and the hurdles it must overcome while executing its plans. The disputes and differences section aims to capture the governing conditions under which citizens are accessing the NID, how access to rights for citizens is operating, and how civil society actors and organizations are engaging with changing digital priorities. The final section on citizens' concerns for privacy attempts to identify existing gaps between inclusion and surveillance, and the issues faced by marginalized and vulnerable people.

1 (DoNIDCR, 2024b: 2).
2 (The World Bank 2016a)
3 (DoNIDCR, 2020).
4 (Buggeland, Ann, 1999).
5 (Gelb and Diofasi Metz, 2017).
6 (Gelb, Alan and Julia Clark, 2013); (Zelazny, Frances, 2012).
7 (NID Portal accessed: Feb 2023).
8 (Albro, Marcus, McNamara and Schoch-Spana, eds, 2012).
9 (Ajana, 2012).
10 (Breckenridge, 2019); (Ziewitz, 2016).
11 (SDG 16, UN, 2015).
12 (Gelb and Metz, 2017).
13 (Interview, 31 October 2022).

II. THE BIRTH OF NATIONAL IDENTITY CARD



In 2010, the government proposed an "integrated" Information Technology Policy 2010 to guide the rapid growth of the digital sector. The aim of the policy was to make technology accessible and inclusive to all by investing in digital public infrastructure and services. However, progress in developing secure digital platforms has been limited. For example, on 31 January 2023, the Nepal Government's cyber system faced a significant "DoS attack", exposing digital vulnerabilities. The Ministry of Home Affairs immediately stated that cyber-attacks against government and private systems were increasing, with attempts to gain "illegitimate access or interrupt services", particularly within government defense, finance, and other important systems.[14] Echoing these concerns, a spokesperson at the Ministry of Communication and Information Technology acknowledged that the bill on cyber-security had been under discussion for a long time. However, it has now come into effect as the National Cyber Policy, 2023. Despite such efforts, Nepal lacks a comprehensive data protection policy. Although digital access has been growing, relevant policy measures have not kept pace. As a result, digital security remains weak, both in terms of "national security" and the protection of citizens' personal data.[15]

Amid ongoing efforts to operate and regulate digital systems, Nepal has initiated biometric identification measures through its NID project. The concept of a national digital identity was first introduced in government policy and programs in July 2009, as part of a broader vision to transition from paper-based systems to e-Governance. The budget speech in that year announced plans to issue a biometric smart card with a photograph to all Nepali citizens. This National ID card was envisioned not only for voting purposes but also for accessing social security benefits and various commercial services.[16]

In 2010, the Cabinet formally approved the issuance of a biometric "smart" card. Subsequently, in July 2011, the government established the National ID Management Centre (NIDMC) to oversee the implementation of the digital identification system and civil registration processes.

With support from the Asian Development Bank, the government announced the pilot of a biometric project worth USD 14 million in 2012.[17] This project, equipped with a Unique Identity number, would be piloted to 110,000 citizens in Panchthar District and 7,000 civil servants in Singha Durbar.[18] Subsequently, the first phase of the plan aimed to cover 15 districts, followed by 25, and then the remaining 35 districts.

Between 2012 and 2015, the project made no progress. It was eventually realized that a new law was needed to anchor the biometric identification program. After the Nepal Constitution was promulgated in 2015, the digitization program gained constitutional footing. Article 15 of the Constitution includes a provision for issuing a record where each citizen must have a "clear" identity. As stated in Article 51(f) (7), an "integrated national identity management information system" would be developed to "manage all kinds of information and data of the citizens in an integrated manner," linking with "the services and facilities provided by the State and with... development plans."[19] The distribution of digital IDs was further linked to citizenship certification, as an eligibility requirement, indicating that only individuals with citizenship certificates will be enrolled.

Building on the constitutional provision, in 2016, the government granted the contract to a French company, Morpho Safran (now Idemia). The award was based solely on a technical assessment, stating that this was the only company "technically eligible."[20]

For the pilot phase, Morpho Safran was tasked with providing 117,000 citizens with a biometric ID within a span of two years. Once the collection of biometric data and personal records was completed, the Department of National ID and Civil Registration (DNIDCR) began printing National ID cards for citizens who were enrolled during the pilot phase in 2018. By that date, the government spending had reached an estimated USD 4,878,698.[21]

Despite the progress made, the legal status of the project was still unclear. In 2019, the project encountered significant controversy for the first time. The main opposition party, Nepali Congress, called for the immediate suspension of ID distribution, questioning its legal status. The party argued that the printing and distribution of the National ID card were "illegal" since no specific Act had been passed outlining the status of biometric ID cards and their intended use.

Nepali Congress MP Dilendra Prasad Badu further accused the government of violating the Public Procurement Act by awarding the lucrative contract to Morpho, solely based on a technical assessment rather than through public bidding for which the legal cap is below NRS 2 million.[22] Seconding Badu, MP Amresh Kumar Singh added that moving forward with the National ID program while the citizenship bill was still under discussion was likely to invite problems in the future.[23]

The Nepali Congress MPs criticized the government's actions. Despite Article 15 of the Constitution, stating that "an Act" would be developed to "manage and implement" the biometric project, no such act had been developed. In response to criticism from various quarters, the government passed the National Identity Card and Civil Registration Act in 2019.

Building on global trends, the Act was

Box 2: About the National ID Card from the Department of National ID and Civil Registration's website: https://donidcr.gov.np/Home/NationalIDDetails

National Identity Card of Nepal is a federal level Identity card with a unique identity number for each person that can be obtained by citizens of Nepal, based on their biometric and demographic data.

The data is collected by the Department of National ID and Civil Registration (DONIDCR), under the jurisdiction of the Home Ministry. The contract to process and deliver the cards was signed in 2018 with IDEMIA.

Upon full implementation, this card is to replace the current "Nepalese Citizenship" and it will be used for National Identity, personal identity, as Voter ID Card and as a Social Security Card through its unique number. This card will not replace other documents like Passport, Driver License.

The project began in the fiscal year 2075/76 [2018/19 AD], with initial distributions in districts like Panchthar and to government employees.

SLOGAN : Technology-friendly, well-governed, and robust service delivery is Nepal's pride; the multi-purpose National ID is our identity.

MISSION : To promote quality public service, peace, security, and good governance through the National ID and Civil Registration Management Information System.

VALUES : Supporting Nepal's Prosperous Nepal, Happy Nepali campaign through technology-based identity and registration systems.

Legal Framework :

To systematically advance the National Identity Card program, strategies like the "National Identity Card Management Strategic Plan 2075" and the "Procedures for Registering Details of Nepali Citizens Eligible for National Identity Cards and Their Distribution, 2075" have been implemented. Following numerous decisions by the Council of Ministers and various ministries, the legal foundation for the program was established with the issuance of the National Identity Card and Registration Act on 28 Fagun 2076 [February 11, 2020].

ENROLLMENT PROCESS : To apply for the National ID Card, individuals must be at least 16 years old and provide the following documents:

- Original citizenship card
- Migration certificate (if applicable)
- Marriage certificate (if spouse's name is not on the citizenship card)
- Passport (if available)

Features

- **UNIQUE IDENTIFICATION NUMBER (UIN):** Every individual is assigned a unique number for life.
- **BIOMETRIC INFORMATION:** Includes fingerprints, facial recognition, and iris scans.
- **DEMOGRAPHIC DETAILS:** Stores personal details like name, date of birth, gender, address, and citizenship information.

Box 3: National ID Card: Stated Goals and Promised Benefits

Based on information from the Department of National ID and Civil Registration (DoNIDCR) and public statements by government representatives, the National Identity Card (NID) is closely linked to the state's vision of nation-building, driven by goals of prosperity and administrative efficiency.

The NID is intended to streamline government services, improve administrative coordination, and reduce identity-related fraud. It supports the broader digital governance agenda by integrating multiple government databases and enabling service delivery through a centralized digital identity.

Stated Benefits of the NID:

- **ADMINISTRATIVE MODERNIZATION AND EFFICIENCY:** With NID, the government aims to modernize public administration by integrating identity data across government systems. Through centralized identity management, it seeks to improve interdepartmental coordination, reduce redundancy, and promote a more efficient bureaucracy.
- **DIGITAL GOVERNANCE AND SERVICE DELIVERY:** The NID is expected to streamline the delivery of government services by providing a unified identity verification mechanism. By linking individuals to service databases more efficiently, the government claims it can reduce duplication, improve targeting of beneficiaries, and ensure smoother access.
- **NATIONAL SECURITY AND FRAUD PREVENTION:** The NID is framed as a measure to improve internal security by creating a reliable, tamper-proof identification system. The use of biometric data, such as fingerprints and iris scans, is intended to reduce the risk of identity fraud, forged documents, and impersonation. It is also positioned as a tool to strengthen national security by enabling accurate identification and tracking.
- **ELECTIONS AND VOTER REGISTRATION:** By integrating biometric verification into electoral rolls, the system is expected to reduce duplication, prevent fraud, and improve the overall transparency and credibility of the electoral process.
- **SUPPORT FOR DIGITAL ECONOMY AND ECONOMIC DEVELOPMENT:** The NID is positioned as a foundational tool for promoting Nepal's digital economy. It is intended to enable secure, verifiable identity for digital banking, mobile payment systems, and e-commerce platforms, thereby facilitating greater participation in digital financial systems.
- **ECONOMIC AND DIGITAL INCLUSION:** The NID is also presented as a pathway toward inclusive economic participation. The integration of all citizens into the digital ecosystem is framed as a step toward ensuring that all citizens can benefit from Nepal's transition to a digital economy.

Box 4: Proposed Multipurpose Uses of the National ID Card

Nepal's NID Card is being positioned as a comprehensive, secure identification system intended to streamline governance by replacing multiple identity documents and connecting citizens to a wide range of public and digital services.

Below are the key proposed multipurpose uses of the National ID card:

- **IDENTITY VERIFICATION AND AUTHENTICATION:** The NID card includes biometric features such as fingerprints and iris scans, as well as a QR code, intended to serve as a unique and verifiable proof of identity.
- **CIVIL REGISTRATION AND VITAL EVENTS:** The NID system is expected to interface with civil registration databases to track life events such as birth, marriage, divorce, migration, and death.
- **LINKING OTHER OFFICIAL DOCUMENTS:** The NID number is envisioned to function as a unified identity reference for issuing and renewing documents such as: Passport, Driving License, PAN Card, Voter ID.
- **VOTER IDENTIFICATION AND ELECTORAL ROLL MANAGEMENT:** The Election Commission plans to integrate the NID database with the national voter roll to ensure accurate and tamper-proof voter identification during elections.
- **PROPERTY AND ASSET TRANSACTIONS:** The NID is proposed as a mandatory document for the registration, transfer, and verification of assets such as: land ownership, vehicle registration and transfers.
- **ACCESS TO SOCIAL SECURITY AND WELFARE PROGRAMS:** The NID will be used to verify eligibility for and deliver services such as elderly allowances, disability benefits, single women's support and pensions.
- **BANKING AND DIGITAL FINANCIAL TRANSACTIONS:** Following a directive from Nepal Rastra Bank, the NID number is now required for opening new bank accounts.
- **TAXATION AND REVENUE TRACKING:** The NID is expected to be linked with tax records, potentially replacing or integrating with PAN numbers, potentially enhancing tax compliance.
- **HEALTH AND MEDICAL RECORD INTEGRATION:** There are ongoing discussions about using the NID to link individuals' health and medical records for easier access to public health services. However, the implications for medical privacy and consent mechanisms remain unclear.
- **BORDER MANAGEMENT AND NATIONAL SECURITY:** The NID system will be integrated with immigration, border surveillance, and internal security.

Box 5: Timeline: Development and Implementation of Nepal's NID System

JULY 2009
The concept of the NID is introduced in the government's policy and budget speech, aiming to use it for elections and social security delivery.

APRIL 2010
A pilot project is launched to issue voter ID cards with photographs and fingerprints, laying the groundwork for biometric identification.

NOVEMBER 2018
Enrollment of NID cards begins in Panchthar district and Singha Durbar as part of the first-phase rollout. The first card was handed over to a 101-year-old woman in Panchthar district.

JANUARY 2019
The National Identity Card and Civil Registration Bill is tabled in Parliament.

AUGUST 2019
Parliament passes the National Identity Card and Civil Registration Bill, formally establishing the legal basis for NID.

NOVEMBER 2021
E-passports linked to NID numbers are issued; the Nepal Telecommunications Authority (NTA) begins drafting terms of reference to link SIM card registration with NID.

APRIL 2022
The government announces that NID will become mandatory for various licenses and official documents in the future.

JUNE 2024
Government announces NID to be mandatory for accessing services such as banking, SIM registration, social security, civil service exams, land and vehicle transactions.

JULY 2024
Nepal's Supreme Court issues an interim order suspending the enforcement of mandatory NID for public services, following criticism over poor card distribution and access issues.

JANUARY 9, 2025
Nepal Rastra Bank enforces a directive requiring the NID number for opening new bank accounts.

JANUARY 19, 2025
The Supreme Court nullifies its interim order, clearing the way for the government to resume enforcing NID requirements across multiple services.

MARCH 2025
Home Minister Ramesh Lekhak declares in Parliament that NID mandate exemptions will apply to specific groups: children, people unable to care for themselves, persons with disabilities, the helpless, and citizens over 90 years old.

APRIL 2025
6.23 million NID cards printed, 2.31 million cards received by applicants

JULY, 2025
The government reverses its earlier decision to require NID for receiving social security allowances, acknowledging significant distribution failures. It announces that benefits will not be withheld due to lack of NID.

JULY 2025
The Nagarik app is integrated with the National ID system, allowing citizens to access their ID details directly through the app.

introduced with two primary objectives: to enhance security and transparency, and to ensure citizens' access to their rights.[24] That same year, the National Identity Card Management Regulations outlined the intended functions of the NID. It was designated as the "primary basis" for accessing all government services, including social security.[25] Additionally, the card would also be interlinked with "certain private services", such as banking.[26]

While implementing this law, the Act states that "personal privacy will be assured".[27] Yet it simultaneously claims that the biometric and personal data collected by the DNIDCR will be used as an integrated system to maximize interoperability. As concerns about data theft and privacy issues grow, a new security space that is not as safe as claimed is already in the making. Body and Data conducted a separate study of this pilot and published a report in 2023, demonstrating that there are "significant gaps" between the promises of digitization and its actual implementation.[28]

The implementation gap is evident, as the NID was launched without sufficient technological assessment and administrative preparedness. In 2018, the government announced its goal to complete the enrollment of all citizens within five years, by 2023. However, by the end of 2024, approximately 16.3 million individuals had been enrolled, with only 1.6 million National ID cards issued. Of these, 1,61,113 NID cards were rejected by users due to "mistakes" in their identifying information.[29]

A NEW SECURITY SPACE

National ID is a foundational element of an emerging surveillance culture. Unlike in India, where Aadhaar enrollment remains voluntary with the goal of accurately identifying beneficiaries for various social sector schemes, in Nepal, National ID is mandatory primarily for digital identification.[30] From the users' perspective, the National ID is seen as an additional layer of bureaucracy and surveillance within an already complex system. Users, who face a complicated application process, expect unequal access to obtaining the NID. Although they recognize its role in customer due diligence, there is uncertainty about which essential services will be linked to beneficiary due diligence.

Historical controversies over Nepali citizenship have left millions of residents without citizenship certificates. Recent disputes concerning children of parents with "birthright" citizenship cards have significantly increased this exclusion. The National ID system is likely to reinforce these inequalities, as its distribution does not address existing social divisions based on caste, class, gender, and ethnicity. Instead, the move to digital identification may create new forms of exclusion and discrimination.

As seen in the *Aadhaar* case in India, existing social divisions tend to be reinforced by such identity systems.[31] In Nepal, a similar pattern is emerging. Several settlements in Sarlahi districts are home to individuals who lack citizenship certificates, rendering them ineligible for NID enrollment. Estimates suggest that this number reaches more than five million nationwide.[32]

In the long run, as reliance on biometric identification grows, the service culture may begin to "normalizing suspicion", with the NID becoming a key surveillance tool. For state actors, it already functions as a means to monitoring and "controlling crime" and "regulating embezzlement".[33] There is optimism among officials that the National ID's digital infrastructure could lay the foundation for a new security landscape.

The government's claims of transparency in relation to the project are being questioned. The national digitization project has once again violated public procurement laws by awarding a high-value contract to Idemia (formerly Morpho) without a competitive bidding process.[34] In 2021, the same French company received a contract to supply an additional 12 million NID cards, also without following competitive procurement procedures.[35]

Idemia touts itself as a "renowned expert in civil identity solutions" globally, managing "the entire identity value chain from citizen enrollment to identity document" production, including upgrading "digital ID ecosystems".[36] Beyond its work in India with Aadhaar, at the time of writing this report, Idemia has undertaken over 100 active projects worldwide, including collaborations with various countries and organizations. Despite controversies surrounding "political influence in securing contracts," Nepal's political class has repeatedly awarded high-value contracts to Idemia merely on technical assessments.

Collaborating with a private company for biometric identification poses challenges to safeguarding citizens' fundamental freedoms and privacy. The design of the Idemia system and its potential privacy infringements remain unclear even at higher government levels.[37] While senior officers at NIDMC believe privacy infringements are unlikely, concerns persist about possible data breaches and privacy violations by private companies like Idemia. Citizens' insecurity often stems from the government's attempts to prioritize commercial interests over fundamental freedoms and constitutional rights. Nepali citizens and civil society organizations appear ill-prepared to address Nepal's political ambition for biometric initiatives, as expressed by many users.

Many people have echoed the sentiment succinctly articulated by a man in Khotang: "This may be intended to make the national system more organized. The National Identity Card seems to simplify various processes, making it more convenient for citizens and even more so for the state. The government benefits significantly, particularly through increased control over its citizens."[38]

14 (Phone-based interview, 27 January 2023).
15 (Quote in Nayapatriak, 2023).
16 (DoNIDCR, 2023b).
17 (Ibid).
18 (Body & Data, 2023).
19 (DoNIDCR, 2023a).
20 (The Kathmandu Post, 2016).
21 (DoNIDCR, 2024b).
22 (Himalayan News Service, 2019).
23 (Ibid).
24 (The Constitution of Nepal, 2015).
25 (The National Identity Card Management Regulations, 2019).
26 (Ibid).
27 (The National Identity Card and Civil Registration Act, 2019).
28 (Body & Data, 2023).
29 (Interview, 12 December 2024).
30 (Aiyar, 2017).
31 (Rao, 2019).
32 (Shrestha and Mulmi, 2016: 13).
33 (Interviews and policy documents).
34 (Morpho Safran was renamed as Idemia in 2017).
35 (DoNIDCR, 2023b).
36 (Idemia Official website, accessed 21 February 2023).
37 (Interview, February 2023, Kathmandu).
38 (Interview, 30 October 2022, Khotang).

III. HOW THE GOVERNMENT IS WORKING

The National ID system operates as a highly centralized program. The role of District Administration Offices has been limited to following top-down instructions to ensure basic implementation. The role of Municipalities has been limited to facilitating the implementation process on the ground. The local government units were not involved in the consultative processes of planning and forming policy, nor in assessing difficulties of digital governance. Their on-the-ground knowledge of digital governance challenges, including gaps in digital literacy and capacity, was largely overlooked. They were not even consulted to measure institutional capacities or assess social contexts that could act as hurdles in a society where digital literacy is low, "smart" governance is a new concept for many, and digital public infrastructure is weak.

The NID system was initiated with the promise of integrating public services through interoperability. Reports indicate that the Department of Immigration, Social Security Allowances Distribution System, Civil Registration System, Company Registration Office, and Pension Management Office have already been integrated to create a digital impact. Integration with the Department of Inland Revenue, Health Insurance Board, Department of Transportation Management, and Nagarik App System has been completed, but operations are yet in effect. The integration of NTC, Ncell and Credit Information Bureau with NIDMIS is currently in progress. However, it is important to note that integration is a new process that has just begun, and its digital interoperability will be tested over time.

Until now, the growing e-governance experiences of public staff have played a crucial role in assisting District Administration Offices, and also Local Governments, in collecting biometric data for National ID cards. Government workforce on the ground have been exposed to e-governance and digital literacy only in recent years. Across the country, the "universal" digital system utilized by almost all Local Governments is the Public Finance Management (PFM) system, commonly known as SuTRA (Sub-National Treasury Regulatory Application). This financial software was developed by the Treasury and Accounts Control Office at the federal level, and is now being utilized by Local Governments. SuTRA was created to facilitate payment release and expenditure tracking, with Local Governments using it for accounting purposes. One of its main objectives is to enhance intergovernmental fiscal relations and increase transparency in public finance. However, without sufficient citizen participation, social audit, effective public audit, the digital accounting system falls short of being truly transparent.

Along with SuTRA, the use of technologies is rapidly increasing within government agencies. The Land Management Office, Survey Department, and Statistics Department across the country have already shifted from "traditional" to digital services. However, digital transformation is far from easy.

A government officer from Sarlahi claimed that the NID program would be a "game changer" in the future, once linked to all governmental services, such as land and revenue, driving licenses, Nepal Telecom, bank accounts, voter IDs, social allowances, and more. He added that people would no longer have to carry different cards for different purposes, making the government's service delivery efficient and ultimately maintaining good governance if effectively implemented. A CSO representative believed that there are no disadvantages to the NID card. He further added, "...it is disadvantageous to frauds and criminals, as they can be tracked using their NID number. It is beneficial for the community."[39]

In the beginning, the DNIDCR created thirty-three positions to steer this operation, with the understanding that additional technical support would be recruited on a contractual basis. In February 2018, the piloting of biometric projects in Paanchthar and Kathmandu proceeded smoothly without much controversy. Following this, in 2018, the mobile station for biometric enrollment began in 15 districts[40] by setting up sixty-two enrollment stations. It was expanded to the next 22 districts.[41] Subsequently, enrollment stations were set up in all districts, except for eleven – Udayapur, Siraha, Bara, Parsa, Ratahat, Sarlahi, Danusha, Dolpa, Humla, Mugu, and Manag.[42] In these remaining districts, the biometric enrollment station for data collection began in 2021, excluding Dolpa, Humla, and Mugu.[43]

When the operation began in each district, the team from Kathmandu organized a day-long orientation program at the district headquarters. Local representatives, Chief District Officers, Local Government officers, political representatives, and journalists were oriented about the biometric projects and their objectives. Additionally, a separate orientation program was held for elected representatives. In each district, along with DAO, there were several mobile camps to collect biometric data from all residents.

In Khotang, seventeen mobile camps operated for a month in 2020 to expedite data collection. During that phase, 126,856 citizens were enrolled to receive ID cards, with

102,587 through mobile camps and the remainder at a biometric station at the CDO office. Due to its population size, Sarlahi had twenty-six mobile camps in operation for four to six weeks in 2021. While 19,272 residents were enrolled through mobile camps, an additional 16,299 were enrolled at biometric stations at the CDO office, by November 2023. By the end of 2024, enrollment had reached approximately 300,000.[44]

By November 2024, out of 16.35 million enrollments, the government had distributed NIDs to 1.65 million citizens. During the card collection process, 161,113 users rejected their cards due to errors in their information.[45] Before reissuing their ID cards, users had to submit a request form to correct the information, which was then confirmed by an operator and verified by a verifying officer.[46] The enrollment for the National ID began in the third phase in 28 out of 77 districts, where the enrollment process was in full swing.

In June 2024, it was reported that the government was receiving data from approximately 4,000 registrations per day. Around the same time, the government had distributed 4,200 card-reader machines in 333 local units across 28 districts to work in conjunction with social security allowances.[47]

The government faced significant opposition in its push to make the use of NID cards mandatory. A writ was filed against this decision leading the Supreme Court to issue an interim order against immediately enforcing the requirement for national identity cards to access public services, including social security allowances. In response to concerns from the public and elderly people, a division bench of Justices Dr Manoj Kumar Sharma and Til Prasad Shrestha issued the order against the decision made by the Ministry of Home Affairs on June 24. They claimed that the government was delaying the issuance of the ID cards.[48]

In an effort to give a mandatory push to its digital identification project, the government is now "informally" providing the National Identity Number (NIN) to newly born children, averaging 2,000 per day.[49] Access to the NIN is required to take the licensing examination at the Nepal Medical Council.[50]

In several instances, registering to obtain ID cards was not as straightforward as it seemed. Due to a lack of essential services in place, the government caused inconvenience for service users. In Sarlahi, users were required to pay anywhere from Rs. 200 to Rs. 500 by cyber operators to complete an online form that was supposed to be free. Many users who had to fill out the form expressed confusion, stating they, "didn't understand why the service wasn't available at the district office and why they had to fill it out elsewhere."[51]

When residents learned or were informed that the service was meant to be free, many complained about the inconsistent pricing. As complaints from end users increased, a significant number of them went as a delegation to the CDO. In response to their concerns about free and fair service, the CDO explained that the office lacked the necessary human resources and administrative capacity to provide free services. Instead, the CDO summoned all the cyber operators to the office to "warn them to charge a nominal fee of Rs. 200 and if they were found overcharging, action would be taken against them."[52]

In case of excessive pricing, users were encouraged to file complaints at the DAO office to take action against cyber operators. Following this, arbitrary pricing was regulated; in the event of overcharging, users could file complaints against cyber operators at the CDO office. It was reported that no such complaints had been filed since then.

Grievances against government inefficiency are widespread, with the following sentiment from users being common:

"People are running illegal businesses in this district under the guise of electronics and digitization. Citizens are being forced to spend a considerable amount of money on these services and are suffering greatly as a result. The government promises easy services through digitization and e-commerce, but people are encountering numerous challenges. Moreover, if someone needs to visit a cyber cafe to fill out a form, they could potentially miss deadlines or struggle to complete the work as government offices have specific times for form submission. A citizen from a rural area may not be informed about these deadlines. How are we supposed to know?"

For citizens, the challenges didn't stop at having limited information, exposing personal data to cyber operators, paying fees for supposedly free services, and spending days outside or making multiple trips just to get enrolled for an NID. Even after overcoming these obstacles, citizens had to wait for hours to submit and verify their applications. The DAO in Sarlahi could only process a maximum of 85 applications daily, while number of applicants exceeded this capacity every day. In Khotang, although the flow of applicants was around 100-120, the capacity to process applications was around 80-85. The waiting process was more organized in Khotang, as the DAO implemented a coupon system early on. The introduction of the coupon system to manage the queue of citizens arrived late in Sarlahi.

With few exceptions, citizens filled out the online form in advance. Operators at the DAO only needed to verify details before capturing a digital photo, fingerprints, and an iris scan; a process that took less than 10 minutes. When elderly or illiterate citizens were in the queue, operators typically assisted them in filling out the form.

Due to poor digital infrastructure, the capacity to process fewer than around 85 applications was further affected by a number of factors. The irregular power supply, system functionality, and material supplies tend to have a greater impact than other issues. A system failure meant all processes were halted until restoration. In both districts it was reported that the online system gets hung at least twice a day. Accessibility and the supply of technical materials were reported to be huge challenges in both districts. Even in places as connected as Sarlahi, minor technical problems or a lack of material supplies would sometimes take days to be fixed, leading to a shutdown of every computer related service. If technical problems were slightly more serious, services would be interrupted for weeks.

Getting enrolled for the National ID does not mean citizens have received their biometric cards. Initially users were told that they would receive their ID cards within six months. However, in Sarlahi and Khotang, where it had been more than 18 months while this field work was conducted, most users have no clue as to why there was such a delay. They have not even checked the whereabouts of the ID card at the ward office or the CDO office. They were not even informed about its status by their local officers or local representatives. Citizens who have inquired about the whereabouts of their ID card have said that even local officers and representatives have "no clue" about the delay, so they are unable to provide specific answers regarding when and how the ID card will be distributed.

The information vacuum highlights the top-down approach of the project, where even authorities at local levels are not informed about the processing status and use of NID. Since the biometric project is conceived, designed, and owned by the federal government, local officers and representatives feel helpless regarding existing delays. The CDO in Sarlahi stated that digital programs are "decided and designed by the federal government" and the role of provincial and local governments is "limited to implementing those programs".[53] He also mentioned that the implementation of online systems at local and provincial levels is restricted, due to limited digital infrastructure and inadequate human resources.

In terms of district level digital programs, LGs are only involved in the implementation process. They are not directly responsible for "developing, updating, or making technologies user friendly," as these tasks are handled at the federal level. The CDO office can utilize the technologies provided by the federal government. However, they often find that the "feedback" from the district level regarding these technologies is not taken seriously by decision makers at the center.[55]

Box 6: NID Administrative and Implementation Structure

The Ministry of Home Affairs (MoHA) oversees the NID system, with the Department of National ID and Civil Registration (DoNIDCR) as the lead implementing agency. The system operates through coordination with multiple national and local bodies:

- DoNIDCR: Executes and manages NID operations—data collection, processing, issuance, and maintenance of the biometric database in compliance with privacy and security standards.
- District Administration Offices (DAOs): Facilitate NID registration, biometric data collection, and card issuance at the district level.
- Local Governments (Wards/Municipalities): Support outreach and data collection, especially for marginalized and remote populations during registration drives.
- National Information Technology Center (NITC): Manages the technical infrastructure, ensures data security, and integrates NID with other e-government platforms.
- Coordination and Oversight: The Centralized Data Management and Security Committee oversees implementation and security, while MoHA and DoNIDCR coordinate inter-agency collaboration for nationwide rollout.

DIFFICULTIES WITHIN

Government officials who support the use of new digital technology believe that, once the system is fully in place, different departments will be able to share responsibility and ownership of it. However, some government staff, especially those in traditional roles, are resisting this change. Many of them either lack the necessary computer skills or struggle to learn how to use digital tools. Because of this, there is an ongoing debate about whether to stick with paper-based systems or switch fully to digital ones.

Chief District Officers (CDOs) from both districts have pointed out another problem. They have noted that some individuals who are involved in financial misconduct are reluctant to support the move to digital systems. These people fear that the transparency of digital records may reveal their unethical actions. As a result, they are slowing down the process of adopting digital technology. Additionally, instances of sabotage to IT systems, such as "cutting off wires" have been reported.[56]

Although the government has shifted to e-procurement measures, the system faces significant challenges due to its lack of robustness. The government lacks the technical human resources necessary for constant maintenance. A senior officer in Khotang pointed out that sending e-procurement to the PPMO is always "problematic". The system is "difficult to manage" due to poor digital infrastructure, including basic elements like wiring systems. The digital tax system in use faces regular problems as well.

Due to a shortage of technical manpower, the Ministry of Finance has to hire outside consultants to manage the system. Many officers in Sarlahi and Khotang reported "constant disruptions", emphasizing that a government lacking the basic capacity to manage a robust digital system will struggle to transition biometric measures.

A senior officer with experience working in tax and ICT systems stated that an "integrated" online system may look good on paper but in reality it is not feasible. He believes that within its current practices, the government will struggle to attract competent human resources. If someone is hired in the IT department, their salary would be equivalent to that of a deputy-secretary. However, their market value and opportunity cost would be higher. Their salary at a government office would be around NRS 40,000, which is lower than what they could earn outside the government. Even if they choose to work for government offices, they are unlikely to stay for long.

Digital administrative promises cannot be efficiently fulfilled through traditional arrangement in public administration. According to the CDO in Sarlahi, the federal government must consider their tech-heavy projects separately to succeed. Without launching separate incentive packages to attract tech-friendly human resources, the officer predicts challenges in implementing digital projects like the National ID.[58] Officers and frontline staff at the District Administration Offices in Sarlahi and Khotang voiced concerns that the federal government's expectations to transition digitally without investing in administrative arrangements and human resources are "unconvincing" and only make their work more difficult. Echoing these concerns, the IT director at the DNIDCR stated that even within his department, the existing workforce holds onto a traditional mindset, hindering the digital transformation. To achieve its transformative goals the government "must create a separate administrative arrangement rather than operating through existing offices."[59]

DIGITAL LITERACY

To truly envision a "Digital Nepal," we must imagine a country where digital systems function smoothly, and both service providers (such as government offices and private companies) and users (such as the general public) can easily utilize technology to access information, communicate, and collaborate. However, achieving this vision is difficult due to numerous existing problems.

Digital literacy is the ability to access, understand, evaluate, and communicate information using digital technologies. It includes skills such as operating devices, managing files, navigating the internet, and using search engines effectively. It also involves assessing the reliability of online content and identifying misinformation or bias, especially on digital and social media platforms.

However, many individuals lack digital knowledge and technical skills, which makes it hard for them to navigate these new systems. There is also a lack of long-term commitment to enhancing and sustaining these digital tools. In Sarlahi district, frequent power outages and computer system failures pose major obstacles. In Khotang, such issues happen so often that people have come to see them as "normal". In both districts, government staff and citizens are just beginning to utilize digital services, and are struggling to fully operate and benefit from them.

A policy on "Digital Nepal" asserts that new technology will "empower citizens by

Box 7: Disruptions in Bishnupur, Sarlahi

Sarlahi is one of the districts where enrollment was delayed due to various disruptions, including a theft of computers from the enrollment station. The incident took place in Bishnu Rural Municipality during a mobile camp. An enrollment station was set up at a building where a bank was located with a security guard present. A group of cadres from oppositional groups, citing that the house was owned by a political leader, opposed getting enrolled. They refused to submit digital and biometric details for the National ID at a private residence. They created problems and tried to disrupt the enrollment process by discouraging people from getting enrolled. The ongoing disruption led to the theft of two computers from the station. With support from the local government, the district office issued several public warnings stating that whoever had stolen the computers should return them immediately, or they would face severe punishment once identified. The public warnings continued for two days through loudspeakers. Eventually, the stolen computers were found in a paddy field, but the culprits were not identified. It was assumed that the thieves had secretly placed them there during the night. The responsible officers retrieved the computers and set them up in the same place. Upon inspection, it was found that the biometric data collected earlier was not damaged. The enrollment process continued, but no individuals were identified as guilty.

According to the CDO, every district and society has its own local work culture and leadership practices. Meeting an enrollment target set at the ministry level is challenging at the district level due to the local context. In addition to the theft of computers, in Sarlahi district, there were challenges in implementing enrollment because data entry operators and office personnel often refused to cooperate. Instead, they pressured the authority, citing political connections or leverage and demanded more facilities and allowances. They were inconsistent in showing up for work and disobeyed orders. Initially, they worked as expected, but gradually became reluctant. These issues delayed meeting the minimum enrollment target at the mobile camps. When the timeline for the mobile camps was 15 days, on the 14th day, leaders from the area visited the district office to request an extension. After several discussions, the CDO made it clear that they would not be paid if basic requirements were not met. Despite repeated postponements, the enrollment work gained momentum thereafter.

During the study, it was observed that even after multiple mobile camps in villages, there was a significant daily queue of people visiting district offices to enroll because they had not been able to do so earlier. They needed the National ID, especially for travel abroad. The CDO noted that there was an assumption that pressure on the DAO would decrease after the mobile camps, but this was not the case. The daily pressure at the CDO office remained high.

enhancing connectivity, increasing the availability of e-services, boosting e-commerce, and creating job opportunities in the digital economy."[60] However, the IT officer at the district office mentioned that digital literacy is a significant issue among users, including within the government system. In Sarlahi, it is estimated that about 70 percent of the district population has access to Facebook and TikTok, but less than 20 percent visit government websites. Civil servants are also reportedly unaware of the digital content available on their office website. The CDO office relies on less trained human resources who are still learning to navigate digital systems, despite efforts to enhance their digital skills.

In society, many private organizations and NGOs are running training programs to help people learn basic skills such as reading, writing, using computers, navigating online portals, and operating smartphones. These efforts aim to improve people's ability to use digital tools in their daily lives.

However, these programs do not operate in a simple environment. They exist within a complicated setting where both social and technological factors can create problems. For example, even if someone learns how to use a smartphone or a computer, they may still face challenges such as poor internet access, lack of local support, or difficulty applying what they learned in real-life situations.

Being "digitally literate" means more than just knowing how to use a device. It also means understanding when it is appropriate to use a digital tool and when it is better to ask for help from another person. True digital literacy combines technical skills with good judgment and the ability to navigate both digital and human systems. Digitally literate individuals need to engage with online content responsibly, understanding its social, legal, and environmental impacts. As digital landscapes are changing rapidly, they also need to commit to ongoing learning, regularly updating their skills to adapt to new digital tools and platforms.

Understanding the network of relevant institutions and being able to confidently communicate with authorities when the digital system is not functioning properly is crucial for meaningful engagement. Civil society and media can play a significant role in this process. However, in both Sarlahi and Khotang, it was observed that journalists and civil society members lacked digital literacy and they were largely uninformed about ongoing digital initiatives in their regions, including the National ID program. They were not adequately equipped to address the concerns and needs of users.

Regular observation can also improve one's ability to comprehend and evaluate digital processes. A lawyer in Khotang, who frequently visits the District Administration Office, shared that he has gained considerable knowledge about technology simply by observing the section responsible for photographs, biometrics, stamps, and form processing. He believes that providing user-friendly promotional material about the importance and usage of ID cards is crucial, as verbal information and one-time orientations are insufficient. He expressed skepticism towards the government's traditional instructions delivered in a rushed manner, stating that "they do not effectively educate users on biometric technology and its applications."[61]

POOR INFRASTRUCTURE

The Digital Public Infrastructure (DPI) is currently very weak, leading to uneven access to unreliable computer networks.

In areas like Sarlahi and Khotang, online networks frequently experience disruptions known as "system failures." ICT staff at DAO encounter "frustrating interruptions" due to gaps in electricity supply. In both Khotang and Sarlahi, the CDO emphasized the necessity of overcoming multiple breakdowns, highlighting the importance of addressing infrastructure gaps and maintenance issues. They also pointed out that while the federal government should prioritize investing in DPI, its focus has mainly been on setting ambitious targets rather than investing in foundational elements.

Poor infrastructure directly impacts the quality of services. In Khotang, there were numerous issues with processing and verifying ID enrollments, often resulting in "system failures" that prevented people from enrolling. Many individuals have to wait in long queues, only to return home without being enrolled. Although a coupon system was introduced to alleviate wait times, technical issues prevented its successful implementation. Limited computers and staff meant that citizens had to pay additional service charges to private computer operators to complete their forms, and then subsequently wait in long queues.

Junior officers repeatedly raised DPI concerns with the CDO, urging urgent action to address technical issues. However, their efforts were not taken seriously and government officers showed little consideration for the problems faced by their subordinates. The CDO cited the challenges of working in a rural area with limited technological resources and skilled personnel, making it difficult to utilize technology effectively.

In Sarlahi and Khotang, mobile stations were set up for biometric enrollment; however, most data collection took place offline before being processed online, resulting in errors in the enrollment data. This highlights the limitations of DPI and the extra burden it places on District Administration Offices, as they need non-technical staff to assist with the enrollment process.

In Nepal, where chronic governance challenges have eroded public trust in state institutions, technical problems are often viewed with suspicion rather than understanding. For example, when services at the DAO in Sarlahi were shut down for three days due to technical issues, many locals doubted the validity of the shutdown, attributing it to corruption or lack of transparent communication. Participants in focus group discussions expressed frustration, with one noting that technical problems were often used as excuses for bribery. Another participant highlighted the lack of transparency, noting that users often cannot distinguish between genuine system failures and excuses masking administrative inefficiencies.

39 (FGD with local CSO, 23 September 2022).

40 Jhapa, Sankhuwasabha, Saptari, Mahottari, Lalitpur, Rasuwa, Chitwan, Tanahu, Sangya, Kapilvastu, Gulmi, Salyan, Jumla, Kanchanpur, and Acham.

41 (Khotang, Okhaldhunga, Solukhumbu, Puthan, Rolpa, Dang, Bake, Bardiya, Kailali, Sunsari, Morang, Dhankuta, Terathum, Bhojpur, Illam, Taplejung, Surkhet, East Rukum, West Rukum, Dailekh, Jagarkot, and Kalikot.)

42 (DoNIDCR, 2024b)

43 (Ibid).

44 (Phone-based interview with IT officer, 15 January 2024)

45 (DoNIDCR, 2024b)

46 (Interview, 12 December 2024).

47 (Bhusal, Thira Lal 2024).

48 (Supreme Court Interim Order 080-WO-1524, Ram Bahadur Raut vs Prime Minister of Nepal)

49 (Shrestha, Prithivi Man, 2024).

50 (DoNIDCR 2023b).

51 (Highlighted in all FGDs in Sarlahi, 23-25 September 2022).

52 (Interviews, 21 September 2022).

53 (Ibid).

54 (Ibid).

55 (Interviews, 22 September 2022 and 30 October 2022, in Sarlahi and Khotang, respectively).

56 (Interviews, 21 September 2022)

57 (Interviews, CDO Sarlahi, ICT officers in Sarlahi and Khotang also second this perspective, 21 September 2022).

58 (Interview, 21 September 2022).

59 (Interview, 12 December 2024).

60 (Government of Nepal, 2010).

61 (Interview, 1 November 2022, Khotang).

IV. DISPUTES AND DIFFERENCES

The National ID

Nepal's National ID system is based on the World Bank's "Digital Identification for Development" (D4D) model. This system is designed to be universal and applicable to all the residents of the country. The Nepal government has mandated this ID for all residents, but in reality, only those with a citizenship certificate can obtain the Digital ID. This poses a big problem as many individuals, especially vulnerable groups like single mothers, struggle to obtain citizenship certificates. As a result, they are excluded from the National ID program and cannot benefit from the services connected to it.

During the enrollment process for the National ID, if someone does not have a clear citizenship record, other documents such as a driver's license, academic certificates, or land ownership papers can be used to help verify their personal information. However, these documents only serve to support or cross-check existing data and cannot replace the citizenship certificate when it comes to actually registering for the National ID.

According to the National ID and Civil Registration Act and its regulations, no government official, whether at the national or local level, is allowed to issue a National ID to anyone who does not have a citizenship certificate.

The Digital ID system is closely linked to citizenship laws and is limited to nationals, so it will not address legislative gaps related to discrimination based on membership. Residents without citizenship certificates are automatically excluded from accessing digital rights and services due to the high entry requirements.

Box 8: Making NID mandatory: Resistance and Reversals

The NID card, envisioned as a central tool for identification and service delivery, was intended to be accessible to all residents. As NID enrollment numbers fell short of expectations, the government began making it mandatory first to obtain e-passports. The government increasingly used mandatory requirements to boost registration. Over time, the NID has been made compulsory for accessing a wide range of public and private services.

A notice published by the Ministry of Home Affairs in the Nepal Gazette (Nepal Rajpatra) in June 2024 made it compulsory to present the NID for services such as opening bank accounts, registering SIM cards, receiving social security allowances, sitting for Public Service Commission (Lok Sewa) examinations, and completing land or vehicle transactions. The card was also made mandatory for people with disabilities, the elderly, and single women receiving social security allowances.

The government faced criticism for enforcing the NID requirement for social security benefits without ensuring proper distribution of the cards. Many eligible individuals had yet to receive their NID cards, creating significant barriers to access.

In response, Nepal's Supreme Court issued an interim order in July 2024, suspending the mandatory NID requirement for accessing public services.

However, in early January 2025, the Nepal Rastra Bank (NRB) issued a directive requiring the NID number to open new bank accounts starting from January 14, 2025. This move was based on the same June 2024 Gazette notice, which financial institutions were instructed to follow. Several major banks began rejecting new account applications without an NID number, leading to confusion among customers.

Later that month, the Supreme Court nullified its previous interim orders, officially allowing the government to move forward with enforcing the NID requirement across multiple services.

Despite this, the government walked back on one key provision: the requirement of the NID for receiving social security allowances. A cabinet meeting in July directed the Home Ministry to take the initiative for not making National Identity Card mandatory for social security allowance for now, considering the difficulties faced by citizens to get the ID card. During a parliamentary session in March 2025, Home Minister Ramesh Lekhak announced that certain groups would be exempt from presenting an NID to access essential services: children, persons unable to care for themselves, individuals with disabilities, the helpless, and citizens over 90 years old.

The government's shifting stance and hasty implementation, without adequate planning or infrastructure, has drawn criticism for creating confusion and distress. The use of fear and pressure tactics to enforce the NID has raised serious concerns about citizens' rights and equitable access to services.

The NID is designed to be a functional identification card with its main objective being the digital identification of all citizens.[62] Once digitized, citizenship status and rights are linked to citizenship certification, allowing interoperability for accessing public services such as land registration, transportation, and social security benefits. It also allows for accessing private services in commercial banks and for official offline use when necessary.[63] For the government, its primary function is to enhance surveillance for public security and crime control, including immigration regulations.

Given Nepal's high rate of labor migration, immigration served as a strategic opportunity to implement mandatory National ID enrollment. In November 2021, when the government made NID compulsory for obtaining passports, the Office of Immigration began requiring a NIN. This added another bureaucratic hurdle to the already complex passport application process. The significant number of Nepali migrants creates a high demand for passports, and the NIN requirement led to a substantial increase in enrollment. While making NID mandatory for foreign travel naturally increased enrollment pressure, but the government was not well equipped to handle the enrollments and distribute NID cards at that pace. In 2021, the mandatory enrollment for NID to obtain passports was introduced at a time when even citizens who had enrolled as early as 2019 had not yet received their NID cards in Sarlahi, Khotang, and other parts of the country.

PENDING VERIFICATION

During the NID enrollment process, many citizens faced a common issue of "pending verification". Their data was unverified for reasons unknown to them. Upon closer examination, the cases with pending verification had two common patterns.

The first pattern was related to longstanding administrative inconsistencies in the distribution of citizenship certification. It is common to find errors and variations in dates of birth and the spelling of last names, particularly among the poor, less educated, and illiterate individuals or among distinctly different ethnic names compared to dominant groups. These variations often result in them being unable to apply or having their online entries rejected with a "pending" status. They are then required to repeat a bureaucratic procedure they have already completed in the past to obtain a new citizenship certificate. This not only adds additional burden for users, but also creates unnecessary strain on the District Administration Office, where there is always a long queue of migrant laborers hoping to obtain a citizenship certificate as a prerequisite to issue a passport. During our visit to the DAO in Sarlahi, the unceasing administrative burden and cumbersome service was starkly visible, among other things, due in part to mismatches between service infrastructure and the volume of residents seeking documents like citizenship certificates and National IDs.

The second pattern emerged from human errors made while filling out forms, as well as from the process used by mobile stations to handle offline applications. If mistakes such as typos or inconsistencies were identified later, the form was automatically marked as "pending." The errors were more common in the case of mobile stations where online verification process was unavailable at the spot, and only when the details were entered online errors were detected later.

In both scenarios, citizens had to restart the entire process to verify and complete their enrollment application.

LACK OF ACCURATE AND ACCESSIBLE INFORMATION

The NID initiative, intended to streamline citizen services and promote digital governance, has largely failed to effectively communicate its purpose, benefits, and implications to the general public. Users, who should be at the center of the project, appear to be either misinformed or entirely uninformed about the actual use of the NID. Government officials at the central level have acknowledged that even higher-level discussions were limited, and the program's hasty implementation left little room for proper public engagement.

The FGDs and interviews with citizens in Sarlahi indicated that most citizens were not properly informed by the authorities about the purpose and usage of the National ID. They were not informed about fundamental questions such as why the NID is needed, what the biometric card looks like, and how the NID system works. In all the FGDs conducted in Sarlahi and Khotang, participants stated that they enrolled for NID because they were told that it was "mandatory" and that NID would replace the citizenship certificate in the future. When asked who informed them that the NID would replace the citizenship certificate, most responses were based on hearsay rather than reliable or official information.

In Sarlahi, unlike in Khotang, some people believed that the National ID would be similar to India's Aadhaar card and would offer various benefits. However, when they were asked who told them about this and what specific information was shared, their answers were unclear and mostly based on rumors. Participants in the FGDs also mentioned that such rumors were deliberately spread to encourage people to register quickly. As one participant put it, "This kind of talk was spread just to make people fill out the forms faster" *[staniyalai chhito bharnako lagi yasto halla chalaye]*.

In all three FGDs conducted with women and marginalized individuals in Sarlahi, it was found that local leaders referenced Aadhaar, assuming people would see an incentive in enrolling immediately. However, citizens later discovered that no additional services would be tied to the NID. Beyond a brief orientation for local staff and officials, and minimal guidance offered at the enrollment station, the government had made little investment in public education or awareness-raising around biometric systems.

Government officials at the central level have acknowledged that end-users are ill informed, largely due to limited deliberation and rushed implementations, even at higher levels. This hurriedness, combined with lack of assessment of digital public infrastructure and basic commitment to education and outreach programs, has shaped a fragmented communication landscape, opening spaces for misinformation.

In both Sarlahi and Khotang, it was found that women were less informed about the NID compared to men. Many women enrolled simply because their male family members took them along or asked them to go. During a FGD with female participants in Godaita, Sarlahi, two women said they were unaware of the NID mobile team, stating, "We are daughters-in-law of this village so we don't know about that." Further discussion revealed that they did not have citizenship certificates, which is why they were uninformed. In Khotang, a respondent described a scenario where an orphan child, who grew up without a family, "might not know the name of their own mother, let alone that of their grandfather and grandmother."

Saying that the National ID is "mandatory for all" is misleading, especially for Nepali residents who can't obtain citizenship certificates due to reasons such as birth or marriage. Nevertheless, the pressure to enroll is strong, and many people are signing up for the NID Cards, even if they do not fully understand it or have limited information.

STANDARDIZING BODIES

Biometric tools being used today are not just meant to record or standardize people's physical features, they can also inadvertently make social inequalities worse. For instance, when such technologies fail to account for the diverse backgrounds and lived realities of different groups, they risk excluding significant portions of society. Rather than relying on "one-size-fits-all" designs that risk entrenching unfair treatment and amplifying existing discrimination, biometric systems should be intentionally developed to promote fairness, inclusivity, and equal access for all.

It has been observed that class and ethnic divisions are being reinforced during the implementation of biometric enrollment. Workers who regularly handle coarse materials, such as sand and iron, or work with different chemicals in paddy fields or factories, have experienced issues with biometric machines not properly recording their fingerprints. The machines often require multiple attempts to recognize the fingerprints of workers who engage in physical labor. In Khotang, it was reported that, "the system has difficulty recording the fingerprints of individuals who work outdoors in the village, especially those in the construction field, who are exposed to cement and sand."

An officer at the DAO office mentioned that, due to the mandate to make the card enrollment mandatory, those with difficult-to-read prints are categorized as having "damaged" fingerprints to complete the process. While temporary fixes, such as applying sanitizers or pressing users' hands together, sometimes help, in many cases the issue persists. When data is marked as "damaged," it can also affect passport verification, as the fingerprints do not align, leading to difficulties in obtaining a passport or even outright rejection.

Many workers worry that as their fingerprints become rougher over time, biometric machines will continue to fail in verifying them. Officers admit they have no lasting solution to this problem, often resorting only to consoling users instead of addressing the root issue.

Citizens who have not been officially identified due to a "pending" status, and those who have difficulty verifying their identity on the spot, often through fingerprints, are frequently excluded. Reports of migrants being unable to travel abroad for employment due to being "not verified" for NID registration because of faded fingerprints or "pending" verification status are increasing.

Respondents also reported experiencing ethnic discrimination linked to the use of biometric technology. In Khotang, for example, many individuals from ethnic communities have been required to undergo multiple rounds of iris scans because the generic technology more easily recognizes the bodily features of dominant groups than those of marginalized ones. Ethnic individuals in Khotang have experienced discrimination, especially verbal, while undergoing multiple iris scans.

Box 9: Key concerns of the PwDs

- Provide government officials with proper training and sensitization to better address the needs of PwDs, as there is a serious lack of sensitivity and awareness among government officials when providing fair and equitable services.
- Regularly organize special outreach camps or enrollment drives to make services more accessible to PwDs, as enrollment centers lack alternative accommodation and communication tools.
- Ensure more grievance redressal options for PwDs when they encounter procedural barriers or face enrollment denials, in order to make the enrollment process more inclusive.

An officer responsible for taking biometric records at the CDO office admitted that there are difficulties in capturing retinal scans of local citizens with diverse features, particularly senior citizens."[64] The officer mentioned that due to the "specific eye features of ethnic individuals, they sometimes need to provide assistance during iris-scans."[65] This issue appears to be more prevalent in Khotang, especially among senior citizens, with no similar issues reported in Sarlahi.

During a FGD with persons with disabilities (PwDs), they highlighted numerous challenges arising from gaps in awareness, infrastructure, technology, and implementation. Many biometric enrollment centers are inaccessible due to the lack of ramps, wider doorways, proper seating accommodations or accessible toilets. Poor public transport accessibility limits their ability to reach enrollment centers. Even when they manage to reach these centers, government staff are often not trained to assist physically impaired applicants in a dignified and informed manner. At the enrollment centers, people with limited stamina or muscular dystrophy struggle to wait in long queues without proper accommodations.

There were instances of mistreatment and discrimination towards PwDs at enrollment stations and the DAO.[66] Many applicants reported "feeling mistreated by government officials" due to their physical and developmental impairment. PwDs, particularly those with physical or developmental disabilities who may move more slowly, described being treated poorly while submitting biometric data. Many deaf individuals struggled to follow instructions or express their concerns at enrollment centers, which lacked sign language support or alternative communication tools such as visual displays and writing aids. Similarly, biometric devices like fingerprint readers and iris scanners do not provide automatic audio feedback, making it difficult for blind and low-vision users to understand the process. Many enrollment centers lack alternative communication tools, making it challenging for deaf individuals to understand instructions or communicate their concerns.

During a FGD with members of the queer community, concerns were raised about the NID card and its potential to exacerbate existing inequalities. One significant issue highlighted by the queer community is the lack of a meaningful consultation system that fails to include the queer community.

Another major concern is the lack of information about how personal data, including sensitive details about gender identity, will be protected. People fear their privacy will be violated, especially if their gender expression does not match their legal gender. Some participants who have already received their NID shared their experience of being asked

invasive questions in public such as, “Why are you unmarried even at the age of 35?”. Being questioned about one’s gender identity, particularly in their hometowns where being out could be dangerous poses the risk of further social marginalization and ostracization. The risk of their gender identity being revealed to local officials who know them personally was also flagged as a serious concern, potentially creating unsafe situations at home.

Many in the community questioned the need for gender categorization on the National ID at all, suggesting a separate document that proves nationality and provides access to public services without defining gender. The current system labels gender diverse individuals as “other”, increasing the risk of discrimination and harassment from government employees. Participants also raised concerns about the limited “other” gender category, which does not reflect the diversity of gender identities and feels like an imposed label. Furthermore, transgender individuals who have not been able to update their legal gender due to financial limitations, lack of resources, or social stigma are forced to carry an ID with an incorrect gender marker. Participants also mentioned that they are worried that having “other” on their NID threatens their confidentiality and privacy. They fear that personal information being misused online in a country with weak digital security could lead to job loss, career damage, and even physical harm for queer individuals.

Box 10: Key concerns of the queer community

- Provide government officials with proper training and sensitization to better address the needs of PwDs, as there is a serious lack of sensitivity and awareness among government officials when providing fair and equitable services.
- Regularly organize special outreach camps or enrollment drives to make services more accessible to PwDs, as enrollment centers lack alternative accommodation and communication tools.
- Ensure more grievance redressal options for PwDs when they encounter procedural barriers or face enrollment denials, in order to make the enrollment process more inclusive.

LACK OF PUBLIC CONSULTATIONS

NID is one of Nepal's largest digital projects, intended to improve efficiency and access to essential services such as public identification, social security allowances, migration opportunities, banking facilities, and more. Each of these services has a direct impact on people's daily lives.

However, when developing its legislation and guidelines, the government did not show commitment to following rigorous and transparent parliamentary deliberations. There was a lack of effort to inform the nation about this project, which is of foundational importance to society. There were no consultations with stakeholders from various backgrounds to increase public ownership or inform citizens. The lack of systematic public consultations and involvement of NGOs during implementation hindered the project's transparency and accountability.

Our consultations with CSOs and CBOs in Sarlahi, Khotang and Kathmandu revealed that government agencies did not provide sufficient information on the National ID. Information on digital identification, biometric data, and the purpose and process of NID was neither effectively produced, nor widely promoted or distributed. The information available on the DoNIDCR website is limited to "frequently asked questions" and only in Nepali. Citing Article 5(3) of the Right to Information Act, 2007 DoNIDC also uploads progress report as "proactive disclosure", but they are not user friendly. Producing and disseminating information still has significant issues. When enrollment began in places like Khotang and Sarlahi, citizens were not adequately informed, contradicting the government's claims of transparency. Millions of residents without access to citizenship certificates were excluded from enrollment, failing the promise of including all residents for digital identification.

Misinformation or the lack of proper information was reported in both Khotang and Sarlahi. Separate consultations with media practitioners, FNCCI members, and civil society actors in both districts reported similar experiences. They were not invited to any public consultations when the enrollment for the National ID started in their districts. They lacked basic information about the digital system and how the digital ID would be used. They highlighted the need for digital sensitization and acknowledged their lack of awareness about the biometric database and its use.

In contrast to Sarlahi and Khotang, consultations with CSOs in Kathmandu, indicated

that, depending on their engagement, orientation and interest people had different kinds of information and various levels of understanding about digitization and the function of the National ID. They also expressed unanimous concerns, questioning how the government would ensure data authentication while maintaining the privacy of individuals in the database. In the absence of public consultations and with the National ID cards yet to be distributed, they expressed confusion about how the digital ID would contribute to transparency and good governance.

During the FGDs with people with disabilities (PwDs) and the queer community, they raised similar concerns. PwDs shared that they were instructed to obtain a National ID card in order to access services, as it was a mandatory requirement, but were not provided with adequate information or guidance. This gave the impression that the government was relying on coercive tactics rather than meaningful engagement and support. They felt that the government is not serious about training public officials to use technology in a way that respects and includes people from all backgrounds. The current system is lacking in sensitivity and awareness toward demographic diversity and the specific needs of the queer community.

Many civil society organizations such as Digital Rights Nepal[67] have expressed strong concerns about the government's attempts to restrict their role in assisting individuals in accessing digital platforms and important public information. This restriction prevents end-users, especially those from marginalized groups, from receiving the necessary support and information they require.

FGDs in Sarlahi and Khotang revealed that the lack of public consultations directly impacted citizens' limited understanding of issues and hindered the active role of CSOs.

The study also found that end-users were largely uninformed about the function of the National ID and the benefits they would receive once the digital ID was implemented. Many were misinformed about the program, as they were led to believe that enrolling for their NID would result in receiving rations or relief funds. Poor communication and the spread of misinformation led them to equate the NID with the Indian Aadhaar program, especially in Sarlahi. These actions emphasize the importance of transparency in disseminating accurate information to promote good governance. The government could have utilized various mediums to provide information and circulated it in different local languages as needed. Collaborating with CSOs would have enhanced outreach and ensured more inclusive and informed public engagement.

62 (DoNIDCR, 2024a)
63 Ibid.
64 (Interview, 30 October 2022, Khotang).
65 (Ibid.)
66 (FGD with people-with disabilities, 20 July 2024).
67 Dignity Post, "National ID Card System: A Misguided Priority," July 2023

V. RIGHT TO PRIVACY

In contrast to Sarlahi and Khotang, consultations with CSOs in Kathmandu, indicated that, depending on their engagement, orientation and interest people had different kinds of information and various levels of understanding about digitization and the function of the National ID. They also expressed unanimous concerns, questioning how the government would ensure data authentication while maintaining the privacy of individuals in the database. In the absence of public consultations and with the National ID cards yet to be distributed, they expressed confusion about how the digital ID would contribute to transparency and good governance.

During the FGDs with people with disabilities (PwDs) and the queer community, they raised similar concerns. PwDs shared that they were instructed to obtain a National ID card in order to access services, as it was a mandatory requirement, but were not provided with adequate information or guidance. This gave the impression that the government was relying on coercive tactics rather than meaningful engagement and support. They felt that the government is not serious about training public officials to use technology in a way that respects and includes people from all backgrounds. The current system is lacking in sensitivity and awareness toward demographic diversity and the specific needs of the queer community.

Many civil society organizations such as Digital Rights Nepal have expressed strong concerns about the government's attempts to restrict their role in assisting individuals in accessing digital platforms and important public information. This restriction prevents end-users, especially those from marginalized groups, from receiving the necessary support and information they require.

Data Governance

The NID system was launched in a context where no comprehensive data protection laws existed. Given the scale and sensitivity of the data involved, it was crucial for the NID initiative to develop and publish a clear data governance framework. Such a framework serves as a foundation for responsible data management by defining protocols for data ownership, secure storage, access control, data sharing, and system interoperability. It also ensures compliance with privacy standards and emphasizes the importance of regular training and awareness to uphold accountability.

However, no such comprehensive data governance framework has been made publicly available. While the government has shared limited information regarding data management and security protocols, these disclosures fall short of the transparency and safeguards expected in handling such high-risk data.

Currently, the NID data is managed through the Integrated Data Management System (IDMS). Data is stored at the Government Data Center in Singha Durbar, with backups maintained at a disaster recovery center in Hetauda. The DNIDCR operates its own server infrastructure, with failover and disaster recovery systems in place. Officials claim that even if the primary system collapses, the data can be fully recovered due to this backup setup.

However, serious concerns remain regarding the government's capacity to manage such a large volume of sensitive personal data. Nepal's digital infrastructure is fragile and government websites frequently go offline[68] or are breached. There is a significant shortage of skilled IT personnel, and the government struggles with low retention rates of qualified professionals[69].

Data Sovereignty

Private companies like Idemia, the French multinational providing technical support for Nepal's NID infrastructure, remain largely invisible in public debates on data governance. A report titled Exposing Idemia: The Push for National Biometric IDs in America not only indicates that Idemia is ever-assertive lobbying for national biometric identification in the global north, but also how a private company such as this is a threat to individual freedom. In an attempt to "acquaint Americans and their elected representatives with Idemia and biometric ID cards," Twila Brase and Matt Flanders write, "current or future augmented identification requirements could negatively impact individual freedom and patient access to medical services".[70] The concern comes from a doubt that any private company that "make the rules" behind the walls can also hold the data hostage.

This is the same private company that is providing all technical support to Nepal's biometric data. If a private company can collect or have access to personal data on Nepalis without consent, like in America, "they also have the power to use that data to interfere in the personal lives and private choices of individuals".[71] Beyond the renewal of the Idemia contract, their potential use and abuse of data demands serious public debates in Nepal.

A joint-secretary at the Ministry of Communication and Information Technology, who was earlier involved in the making of the National ID bill, accepts the fact that while the government is capable of ensuring physical security and secure data access, "it is technically not well-equipped to develop its protection system". If such a situation remains for long, as stated by the officer, "growing interference in the personal lives and private choices of Nepalis" would invite many problems in the future.[72]

Gaps in Communication, Training and Education

Beyond technical capacity, there is a troubling lack of awareness and sensitivity regarding data privacy and protection. Government authorities have repeatedly demonstrated poor understanding of data vulnerabilities and shown negligence in handling personal information. For instance, both the Department of Transport Management (DoTM) and the Election Commission have, in the past, published sensitive personal data on their websites, exposing citizens to serious privacy risks[73].

During fieldwork, it was found that even staff at DoNIDCR are not clear on how privacy and security controls are built into the NID technology and its processes. Despite claims of a "secured approach," even basic, high-level information about how the system functions has not been adequately communicated. A section officer responsible for data verification at DoNIDCR mentioned that even officers at his level are not properly educated, trained, or sensitized regarding information and communications technology (ICT). The connection between the secure mode of biometric data and its public uses has not been effectively conveyed to those who need to understand it better.

Internal consultations and communications within DoNIDCR, especially regarding the design and implementation of outreach and education efforts during the rollout of the NID, were found to be minimal. Proactive consultations and communications to design and implement outreach and education campaigns were as limited as they could be.

During fieldwork, it was found that, due to a lack of systematic outreach and information campaigns, users had a very low level of digital literacy. No transparent communication about privacy, data protection, or the uses of these systems was provided. Most people were either unaware of or had little understanding of the privacy risks associated with the personal data they had submitted. They reported submitting biometric details simply because they were asked to, without knowing the purpose or potential uses of that information. Many had never considered the risks of privacy breaches, expressing confusion about how various controls might help mitigate such risks. Others were skeptical and "had a feeling" about data risks but "did not know how to put it into words."

In the past, and even now, it was common to give one's Citizenship Certificate to family members, trusted friends, or neighbors when needed. The sharing of this foundational document spanned all kinds of official uses, setting up small enterprises, purchasing property, taking loans, or joining community groups. Because of such practices, for many users, sharing personal information, even digitally, is considered "normal." At the same time, many also recounted how such sharing had led to violations of rights, including loss of property, unauthorized access to personal data, and interception of official correspondence.

During a consultative meeting with civil society representatives, a member expressed concern about safety and privacy, noting that the government had not provided enough information about data privacy, data security, and its public use. FGDs in Sarlahi and Khotang revealed that there had been inadequate dissemination of information about biometric data collection and data protection, indicating that people were being enrolled without a basic understanding of data privacy and security.

The absence of communication and education efforts to engage the public on privacy and data protection issues raises questions about the intended uses of the NID system and whether it truly empowers individuals with meaningful control over their personal data.

Vulnerable citizens and marginalized communities

Those already vulnerable and marginalized are likely to face more threats to their privacy and fundamental freedom. Inhabitants of both Khotang and Sarlahi go abroad to work in high numbers. Due to their precarious living conditions, migrants and vulnerable people have a history of storing their personal records and documents poorly. Documents are often in bad order, condition, or have incorrect records. These practices have already been linked to exploitation and abuse by agents and private companies, added with pre-required submission of personal documents, including travel ID such as a passport.

With the additional requirement for digital ID, migrants and vulnerable are once again forced to rely on private cyber cafes to fill enrollment forms. To fill digital forms for citizens, several application processing centers and/or cyber cafes are usually located nearby CDO offices and immigration offices. The privacy risks are enormous as the poor and vulnerable are forced to rely on these private services, where their personal information is instantaneously accessible to third parties. Instances where migrant workers realize that they have been cheated, sold, or subject to abuse, only on arrival at their foreign destination, but because they had earlier submitted all their personal information without confirming the details of their employment are plenty.[74] Also, there are many examples of sim-card users having their personal information used against them because they shared it without being cautious. While this exploitation seems to have been "normalized" in Nepal's public life, several outgoing migrants said that forcing them to submit their personal information at random cyber cafes has put their lives at additional risk.

These enormous security risks need to be immediately checked by providing free and secured enrollment services. However, the government's "rush" to implement the national ID project, without enough preparation and adequate resources has continuously created openings of privacy violations, as citizens are once again exposed to unsafe data sharing.

While districts like Sarlahi are recording several cases of cyber-crime, in smaller hill towns like Dikhtel in Khotang, instances of cyber-crime are relatively low. A lawyer in Khotang mentioned, such cases are not even recorded here. Only cases like someone berating someone on social media, or publicizing someone's personal information are recorded, and these cases are very limited in number. He further explained that, "maybe because the cases of cyber-crimes are not registered in the district office, we don't see them often; instead they are registered as cases of indecent behavior, where depositing bail and setting a court date to reach an agreement to not repeat indecent behavior is the norm". He added, "the person is let free like that because there is no mention of the nature of the cyber-crime in a written form." A case of indecent behavior would entail swearing, usage of abusive language, bad treatment, etc. and these are resolved by facilitating an agreement between the two parties with a promise to not repeat this kind of behavior again."

Queer communities have expressed significant privacy concerns regarding the NID system, highlighting the risks it poses to

their safety and dignity. Participants during a FGD noted the lack of meaningful consultation with women and queer individuals, as well as inadequate protections for sensitive personal data such as gender identity. The requirement to disclose gender, especially through the limited and stigmatizing "other" category, was identified as a major source of risk, potentially leading to discrimination by government officials and society at large. Participants emphasized that in a country with weak digital security, the misuse of such information could result in job loss, career setbacks, and even physical harm, underscoring the urgent need for a more inclusive and privacy-respecting approach to the NID system.

Security vs. Privacy

One of the stated purposes of the NID is to support national security, including through enhanced tracking and surveillance. While national security is important, it is often used by governments as a justification for overreach, potentially compromising citizens' privacy.

The legal framework in Nepal recognizes the right to privacy but leaves room for exceptions "in accordance with the law," especially during emergencies or for reasons of national security. This legal ambiguity becomes problematic when biometric technologies are deployed without adequate checks. Privacy rights of citizens are often compromised or ignored, especially during

times of crisis or in the name of "national" security. The Privacy Act Nepal 2018, also provides exceptions to privacy rights during emergency security checks, health treatments, health examinations, disaster management, and authorized interceptions. National Cyber Security Policy, 2023 and ongoing Social Network Bill, 2025 have further complicated the landscape by introducing criminalization measures and broad national security provisions that risk infringing on individual privacy. Due to these loopholes, citizens are forced to prioritize their security over privacy, creating a complex situation, particularly for disadvantaged and vulnerable individuals and groups.

For example, voters' privacy was jeopardized by the Election Commission citing "public disclosure" and "transparency".[75] Body & Data's analysis of privacy laws explains these loopholes that violate the privacy of women, children, or people with disabilities in the name of health emergencies, treatments, or women's privacy in legal proceedings such as divorce cases. In cases where women's sexuality is stigmatized, their privacy regarding sexual health, STIs, or pregnancy/abortion must be protected at all costs, as the impact could be severe among vulnerable groups.

Given that our laws are patriarchal and contain loopholes, the use of biometric information authorized by law and justified by security or development narratives can jeopardize vulnerable groups. Narratives of security and development should not come at the expense of the rights, security and freedom of disadvantaged and vulnerable individuals and groups.

There is the urgent need for a comprehensive privacy and data protection law. As technology becomes more powerful, pervasive, and intrusive, the vulnerability of individuals' privacy continues to grow. Laws must be updated to reflect this new reality where biometrics has emerged as a defining technological development in Nepal. From immigration offices to smartphones, both public and private sectors are increasingly using biometric tools for human identification and recognition. Promoted as means to enhance security and improve service delivery, these technologies are rapidly becoming integral to daily life.

The promise of biometric technology lies in delivering better security and more efficient services. As this technology becomes more economically viable and technically advanced, its adoption will likely transform how Nepalis interact with an expanding digital world shaped by personal data.

As Nepali society becomes more entangled in digital connectivity, it is imperative that we also learn new ways to respect the privacy and dignity of our fellow citizens. The country must intensify its efforts to safeguard individual privacy and freedom in the face of these emerging technological realities.

68 Ekantipur. 2025. Government website started to be closed. July 13 2025.
69 Ekantipur. 2025. 10 out of 15 engineers leave jobs, national ID work disrupted. January 17 2025.
70 (Brase and Flanders, 2018, accessed 2 March 2023).
71 (Ibid.)
72 (Interview, 15 September 2022, Kathmandu).
73 The Right to Privacy in Nepal: Is the Government Upholding It? Medium, July 18 2023.
74 (Baniya et al, 2023).
75 (The Kathmandu Post, 2022).

VI. MOVING FORWARD

The focus of this report has been on the processes of designing the NID, its legislative measures, implementation practices, and citizens' concerns. Body & Data found that Nepal's National ID program reflects an ambitious effort to improve governance and improve access to public services through digital systems. However, as this report has shown, the process remains deeply flawed in its current form. Weak governance structures, inadequate consultation with stakeholders, insufficient transparency, and fragile digital infrastructure have undermined the program's stated goals. Particularly concerning are the risks to privacy, dignity, and safety of marginalized groups, including women, people with disabilities, and queer communities, who face systemic exclusion and heightened vulnerabilities under the current design.

The absence of a comprehensive data protection law and the reliance on centralized biometric databases raise pressing questions about security, accountability, and human rights. Without robust safeguards, the promise of efficiency and inclusion risks being overshadowed by the reality of surveillance, coercion, and discrimination.

Moving forward, the success of the NID system will depend on the government's willingness to center rights, transparency, and meaningful participation in its approach. Inclusive consultation, stronger legal protections, and an unwavering commitment to equity are essential to ensure that the NID becomes a tool for good governance and empowerment rather than surveillance and exclusion.

Building on the previous work and recommendations by Body & Data (see Box 12), the report proposes a range of recommendations, from broad to specific, for the government, private sectors, and civil society organizations.

RECOMMENDATIONS FOR THE GOVERNMENT

The National ID system has been introduced with the stated goals of improving government efficiency and enabling financial and digital inclusion. However, our study finds that these objectives are being undermined by weak governance structures and ineffective implementation. There is a clear lack of commitment to inclusion, and limited transparency or willingness to ensure accountability in the system's design and rollout.

Based on these three standpoints, governance, accessibility and accountability, we offer the recommendations to the government, private sector, and civil society. By addressing the recommendations urgently, Nepal has the opportunity to build a digital identity system that is secure, just, and truly transformative for all its citizens.

1. Ensure a universally accessible foundation for the Digital ID system:

The current National ID system, designed as a digital identification tool linked with civil registration and social security, has not been inclusive. It is issued only to individuals who possess a citizenship certificate, thereby automatically excluding millions of residents from access to digital services. Unlike the citizenship card, the NID is intended to serve as a digital foundation for service delivery, not as proof of citizenship. However, by tying it to citizenship eligibility, the system creates unequal and discriminatory access to digital services. The government must make the NID genuinely accessible to all residents, regardless of geography, language, or socio-economic status. Enrollment centers should be physically accessible to persons with disabilities and equipped with support in local languages, sign language, and visual aids to guarantee equitable participation.

2. Build a robust digital public infrastructure (DPI):

The National ID system marks a significant milestone in developing DPI for service delivery. However, it requires a solid groundwork of infrastructure and systems. The government's ambition to deliver services through a digital ID requires reliable connectivity, secure interoperable systems and skilled human resources. A top-down push for digital transformation, without investing in foundational infrastructure, will not improve efficiency, accessibility, or security.

3. Enact strong legal and policy frameworks:

Nepal must introduce comprehensive privacy and data protection legislation that clearly defines the purpose, limitations, and safeguards for data collected under the NID system. The legal framework should evolve in parallel with technological deployment to ensure adequate protections. Currently, the NID is governed by the National Identity Card and Civil Registration Act, 2020, which provides only limited guidance. The government must urgently enact robust legal safeguards before scaling up the adoption and integration of the NID system. Prioritize legislation that clearly defines limits on data use, mandates informed consent, prohibits surveillance-oriented practices, and introduces strong penalties for misuse.

4. Implement ethical and secure data governance:

The National ID system collects and manages highly sensitive personal and biometric data, making ethical and secure data governance a critical priority. This

should include strong data protection policies, purpose limitation, meaningful user consent before data is shared or repurposed, independent oversight mechanisms, strict access controls and robust authentication protocols to prevent unauthorized access or breaches. Data sharing with other government agencies, such as for passports, voter registration, or social security, must follow limited and regulated pathways, ensuring that data is shared only when necessary and under clear accountability mechanisms.

5. Ensure secure interoperability, inter-agency coordination, and institutional clarity:

NID DPI must support secure, interoperable systems that enable real-time identity verification and service delivery across government agencies. Current efforts remain fragmented and lack a cohesive governance framework. Interoperability should be guided by strong data governance principles, with clear inter-agency coordination and defined mandates, institutional clarity on data management authority and technical protocols, security and privacy safeguards to prevent misuse or unchecked surveillance, Interoperability must enhance public service delivery while protecting individual rights, not serve institutional convenience at the cost of accountability.

6. Build a skilled, sensitive, and inclusive public workforce:

Our research finds that many public servants lack essential training in both technical skills and social sensitivity. For effective and equitable digital service delivery, government institutions must invest in sustained capacity-building. This includes training in digital tools, privacy protocols, and data protection, along with orientation on working with diverse populations and understanding the social realities of digitally underserved communities. Targeted programs must also focus on fostering sensitivity and empathy, ensuring that officials engage marginalized groups with respect and dignity. Participants from these communities reported being ill-treated and disrespected by staff, highlighting the urgent need for training on respectful communication.

7. Strengthen digital literacy and embed digital rights education:

To strengthen digital literacy, the government should adopt a long-term, multi-level approach that goes beyond one-time orientations. Digital literacy programs should address not only basic skills, such as using smartphones, computers, and online portals, but also critical abilities like evaluating online information, recognizing misinformation, and understanding the social and legal implications of digital engagement. Digital literacy and digital rights education should be integrated into school curricula. To overcome barriers such as poor internet access and frequent system failures, the government should pair training with infrastructure improvements, user-friendly materials in local languages, and reliable technical support. Women and marginalized communities should be meaningfully included in outreach and training efforts, with programs designed to reflect their specific needs and contexts. Collaboration with civil society, media, and private organizations can amplify outreach and make learning more accessible. Most importantly, continuous monitoring and refresher programs are necessary to ensure people remain updated as digital platforms evolve.

8. Foster transparency and public consultations:

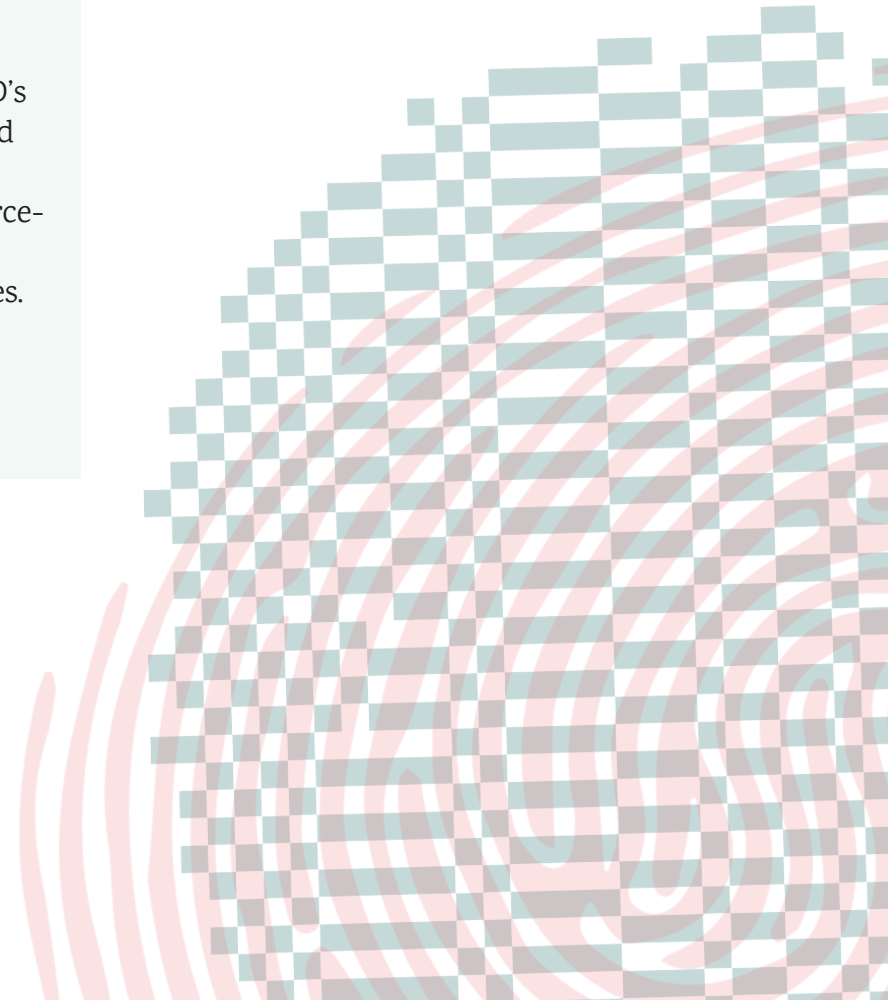
The current implementation model of NID lacks transparency. System designs, procurement processes, and vendor contracts, especially those involving private and foreign technology firms, should be made publicly accessible. Equally important is the inclusion of diverse stakeholders, including CSOs, domain experts, and communities affected by digital exclusion, in meaningful consultations throughout the design and deployment process. Publish procurement contracts, vendor details, and system design frameworks, especially given the involvement of foreign technology firms. Provide regular public reports on data handling, breaches, and oversight findings.

9. Establish independent oversight and grievance mechanisms:

Robust and independent oversight mechanisms are essential to ensure that the NID system operates with integrity and accountability. Regular audits of the NID's infrastructure, operational practices, and data handling must be conducted and publicly reported. There should be enforceable legal provisions for data misuse, unauthorized access, or security breaches. Additionally, accessible and effective grievance redress mechanisms must be established.

10. Ensure NID is a voluntary choice, not a mandatory requirement:

If the NID is meant to improve access and convenience, it must be presented and implemented as a voluntary, beneficial system. People should be informed of its benefits and allowed to participate through informed consent, not compelled through pressure or fear. The government must deliver a thoughtful, and people-centered rollout that respects individual autonomy and builds trust in the system.



Box 12: Recommendations from Digitization of Identity in Nepal: Efforts, Experiences, and Effects

Based on the 2021 pilot study on the NID, Digitization of Identity in Nepal: Efforts, Experiences, and Effects, Body & Data had made recommendations directed at Nepal's policymakers, civil society organizations, and researchers. As the NID system continues to expand, it is important to revisit and reinforce these recommendations in light of growing concerns over data governance, inclusion, and human rights.

We emphasized that Nepal's policymakers should acknowledge that mandatory national digital ID systems collecting excessive amounts of personal demographic and biometric data from citizens must have robust governance and accountability protocols in place to protect the human rights of individuals, especially those from marginalized communities.

Along with strict governance standards, the government must adopt a strategic communication policy that credibly and completely informs all aspects of the program to prevent misinformation. Biometric-based digital ID systems often reinforce deep-rooted socio-cultural exclusions, disproportionately affecting marginalized communities. Therefore, we recommend that no individual be denied access to public services based on possession of a digital ID.

Recommendations for researchers and civil society organizations

- Follow up with an in-depth, mixed-methods study
- Collaborate with other civil society organizations working on digital rights
- Collaborate with other CSOs working at the intersection of social justice and digital policies
- Engage with government and private sector actors to inform about grassroots challenges

Recommendations for policymakers

- Adopt fair, accountable, and transparent digital policymaking and governance processes
- Protect data and digital privacy of citizens
- Ensure robust cybersecurity standards and protocols
- Reevaluate the use of technological solutions
- Create a national digital literacy mission

RECOMMENDATIONS FOR THE PRIVATE SECTOR

In Nepal, the private sector has played a commendable role in laying the groundwork for digital public infrastructure (DPI), including proactive efforts in advancing digital literacy programs. However, there have also been instances where private actors have avoided accountability, undermining trust and rights-based practices.

Given that the NID, digital governance, and digital service delivery are still in their early and vulnerable stages, private companies must play a constructive role in supporting the government and civil society.

11. Uphold ethical data practices:

Private sectors must adopt data practices that prioritize user rights and prevent harm. This means enforcing strong data protection standards, purpose limitation, and robust security across all stages of data handling. Companies should avoid exploitative practices such as unauthorized surveillance or data monetization and provide clear, accessible privacy policies in local languages. They must disclose how NID-linked data is used and shared, and offer opt-out options for NID-based authentication without restricting essential services. They should also prepare for data breaches with effective response plans and timely communication with affected users. Companies must refrain from using NID data for profiling, scoring, or targeted advertising without meaningful consent and resist state demands for mass surveillance or backdoor access that threaten privacy and fundamental rights.

12. Design for inclusion and responsible innovation:

Services linked to the NID must be accessible to all, including people with disabilities, rural communities, and those with limited digital literacy. Companies should avoid making NID the sole access point, with alternative verification methods available to prevent exclusion. Businesses handling sensitive data should avoid deploying high-risk technologies, such as fingerprint or iris scans without clear accountability mechanisms.

13. Contribute to public awareness and collaborate for safeguards:

Private sector actors can contribute to public awareness and digital rights education initiatives. They can integrate user education into their service onboarding processes to help individuals understand their rights, consent, and data use. Companies should collaborate with governments, civil society, and academia to co-develop data protection frameworks, open standards, and ethical guidelines.

RECOMMENDATIONS FOR CIVIL SOCIETY

Civil society and varieties of its organizations play a vital role in shaping rights-based digital governance and ensuring that the NID system does not exacerbate exclusion or violate privacy. As the NID system expands, civil society must act as watchdogs, advocates, and facilitators of public understanding.

CSOs in particular should work alongside vulnerable groups to ensure that the NID system upholds the principles of data privacy, consent, and non-discrimination. This includes holding government agencies and private actors accountable for how personal and biometric data is collected, stored, and engaging in legal and policy advocacy to embed privacy and human rights in the foundation of digital ID governance

14. Advocate for rights-based legal and policy frameworks:

Civil society in general, and CSOs in particular, should advocate for comprehensive tech policies that prioritize privacy, data protection, and uphold human dignity and equity in digital governance. This includes advancing data protection legislation grounded in international standards, promoting safeguards against surveillance, profiling, and algorithmic discrimination, and ensuring that digital identity is not mandatory for accessing essential public services.

15. Strengthen digital literacy and digital rights education:

CSOs can serve as vital partners to the government in empowering communities, especially marginalized groups, through digital literacy initiatives. These programs should explicitly integrate digital rights education, ensuring that citizens not only gain the skills to participate in digital systems but also exercise agency in holding the government and service providers accountable. They should raise awareness about the implications of linking the NID with essential services, and provide clear information on available recourse mechanisms for those who experience exclusion.

16. Facilitate evidence-based public discussions & center lived experiences:

CSOs should lead informed dialogue on the risks and opportunities of digital ID systems by organizing public forums, media engagements, and academic collaborations to foster critical debate. These discussions must prioritize and amplify the lived experiences of marginalized individuals who face barriers to NID access or suffer harm from digital exclusion.

17. Monitor implementation and report harms:

Civil society should act as independent watchdogs to ensure that the NID system upholds principles of equity, accountability, and human rights. Through social audits and community-based monitoring, they can identify and document patterns of exclusion, discrimination, or surveillance.

18. Build coalitions and cross-sector partnerships:

To address the multi-faceted and complex impacts of the NID, CSOs should build strong coalitions and collaborate with media, technologists, lawyers, researchers, and digital rights networks. It is equally important to foster regional and international partnerships to understand and champion digital rights issues. Understanding and advocating for digital rights is becoming increasingly complex and urgent.

REFERENCES

Aiyar, Shankkar. 2017. Aadhar: A Biometric History of India's 12-Digit Revolution. Chennai: Westland Publications.

Ajana, Btihaj. 2012. Biometric citizenship. Citizenship Studies 16 (7): 851–870.

Albro, R., G. E. Marcus, L. McNamara and M. Schoch-Spana, eds. 2012. Anthropologists in the Securityscape: Ethics, Practice, and Professional Identity. Walnut Creek, CA: Left Coast Press.

Baniya, Jeevan, Sanjita Shrestha, Sadikshya Bhattarai, Dogendra Tumsa, Bipin Upsdhyaya, Rajeb Neupane and Prasansa Thapa. 2023. Unscrupulous Recruitment And Precarious Employment of Nepali Migrant Workers. Kathmandu.

Bhusal Thira Lal. 2024. National ID number is sufficient; you don't need a hard copy. Interview with Yubaraj Katel. https://kathmandupost.com/interviews/2024/06/16/national-id-number-is-sufficient-you-don-t-need-a-hard-copy

Body & Data. 2022. Nepal's Biometric National Identity Card: Experiences and Expectations from the Community. Kathmandu.

Breckenridge, K. 2019. The Global Ambitions of the Biometric Anti-Bank: Net1, Lockin and the Technologies of African Financialisation. International Review of Applied Economics 33 (1): 93–118.

Brase, Twila and Matt Flanders. 2018. Exposing Idemia: The Push for National Biometric IDs in America. Policy Insights, February https://www.cchfreedom.org/files/files/Policy%20Insights%20-%20Idemia.pdf (accessed 2 March 2023).

Buggeland, Anne. 1999. Citizenship, Tenancy Rights and Identity: The Case of the Santals/Satars of Jhapa. In Nepal: Tharu and Tarai Neighbours. Harold O Skar, ed., pp. 97-117. Kathmandu: Bibliotheca Himalayica.

DoNIDCR. 2024a. Annual Progress Report (Fiscal Year 2023/24). Kathmandu: Department of National ID and Civil Registration (DoNIDCR).

DoNIDCR, 2024b. Second Quarterly Report of Department of National ID and Civil Registration 2024/25 [In Nepali]; https://donidcr.gov.np/Files/DOC-1be14c7d3-7216-445b-898a-a845ffd2de27.pdf (accessed 27 December 2024).

DoNIDCR. 2023a. FAQ: National ID. https://donidcr.gov.np/Home/NationalIDFaq (accessed 21 February, 2023).

DoNIDCR, 2023b. First Quarterly Report of Department of National ID and Civil Registration 2024/25 [In Nepali], (accessed 27 December 2024).

Fuller, Gillian. 2003. Perfect Match: Biometrics and Body Patterning in a Networked World. Fibreculture 2 (1): http://one.fibreculture- journal.org/fcj002/print

Gelb, Alan and Anna Diofasi Metz. 2017. Identification Revolution. Can Digital ID be harnessed for Development? Center for Global Development.

Gelb, Alan and Julia Clark. 2013. Identification for Development: The Biometrics Revolution. Washington, DC: Center for Global Development, Working Paper 315.

Government of Nepal. The Privacy Act 2075 (2018), Pub. L. No. Act Number 14 of the year 2075 (2018).

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

Himalayan News Service. 2019. Govt told to halt distribution of National ID cards. The Himalayan Times, https://thehimalayantimes.com/nepal/government-told-to-halt-distribution-of-national-id-cards, (accesses 21 February 2023).

Lal, Abha. 2022. Nepal's Biometric Future. Himal South Aisan https://www.himalmag.com/biometric-future-identification-nepal-2022/ (accessed 2 March 2023).

Lebovic, Nitzan. 2015. Biometrics, or the Power of the Radical Center. Critical Inquiry 41(4): 841-868.

Maguire, Mark. 2009. The birth of biometric security. Anthropology Today 25 (2): 9–14.

Pandey, Romkant and Suresh Bahadur Diyal. 2023. A Study on the Situation of National Identify Card in Nepal: implications and challenges. Educational Journal 2(2): 10-26.

Rao, Ursula. 2019. Re-Spatializing Social Security in India. In Spaces of Security, edited by S. Low and M. Maguire, 231–252. New York: New York University Press.

Sigdel Santosh. 2023. National ID Card System: A misguided priority. https://www.nepallivetoday.com/2023/06/29/national-id-card-system-a-misguided-priority/

Shrestha, Prithivi Man. 2024. Digital identification to be assigned during birth registration. The Kathmandu Post, March 4, https://kathmandupost.com/national/2024/03/04/digital-identification-to-be-assigned-during-birth-registration, accessed 9 January 2025.

Shrestha, Sabin and Sabin Mulmi. 2016. Legal Analysis of Citizenship Law of Nepal. Kathmandu: Forum for Women, Law and Development (FWLD).

The Kathmandu Post. 2024. Ideate before implementing [editorial]. https://kathmandupost.com/editorial/2024/08/21/ideate-before-implementing

The Kathmandu Post. 2024. Government backtracks on plan to make National ID cards mandatory for social security allowance. https://kathmandupost.com/national/2024/07/11/government-backtracks-on-plan-to-make-national-id-cards-mandatory-for-social-security-allowance

The Kathmandu Post. 2024. Digital identification to be assigned during birth registration. https://kathmandupost.com/national/2024/03/04/digital-identification-to-be-assigned-during-birth-registration

Dignity Post. 2023. National ID Card System: A misguided priority. https://www.dignitypost.com/news/2023/07/68

World Bank. 2016a. World Development Report 2016: Digital Dividends: Overview. The World Bank Group.

World Bank. 2016b. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation: A joint World Bank Group – GSMA – Secured Identity Alliance Discussion Paper. GSMA, World Bank Group and Secure Identity Alliance.

Zelazny, Frances. 2012. The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries. CGD Policy Paper 008. Center for Global Development, Washington. https://www.cgdev.org/publication/evolution-in- dia%E2%80%99s-uid-program-lessons-learned-and-implications-other-developing

Ziewitz, Malte. 2016. Governing Algorithms: Myth, Mess, and Methods. Science, Technology, and Human Values 41 (1): 3–16.

Body & Data

NEPAL'S BIOMETRIC PRESENT: GOVERNANCE, ACCESSIBILITY & ACCOUNTABILITY

Body & Data is a digital rights organization in Nepal that works towards creating accessible, safe, and just digital spaces for all.

bodyanddata.org