



USAID
FROM THE AMERICAN PEOPLE



EngageMedia



Internews
Local voices. Global change.

State of Digital Identification Systems in South and Southeast Asia

AUGUST 2023

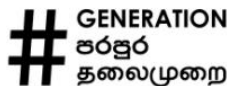



In collaboration with

digitally right



SOCIETY FOR
PEACE&DEMOCRACY





EngageMedia is a nonprofit that promotes digital rights, open and secure technology, and social issue documentary. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights.

Learn more at engagemedia.org.


Digitally Right aspires to support independent media, civil society and business organizations with critical knowledge and solutions to adapt to the rapidly changing information environment. We envision a society where the people of Bangladesh can access information safely and express themselves freely in the digital space.

The Cambodian Center for Independent Media (CCIM) envisions a Cambodian society where everybody is well-informed and empowered to strengthen democratic governance and respect for human rights. CCIM believes that a well-informed Cambodian society will expect and demand good governance, and select leaders that will shape the society and economy in a way that will benefit the Cambodian people equitably.

Southeast Asian Freedom of Expression Network (SAFEnet) advocates for victims of digital rights violations and for Internet policies to include human rights perspectives. SAFEnet's vision is the realization of a digital space that upholds human rights values for all.

Society for Peace and Democracy is a non-government organization that empowers communities through awareness-raising and capacity-building to act and to participate in their own development. Through education and training, the organization develops knowledge and skills, providing opportunities to advocate for improved policies to ensure human rights, inclusion and collective actions.





Digital Rights Nepal is a not-for-profit initiative dedicated to the protection and promotion of digital rights in Nepal. It focuses on digital rights issues such as right to online freedom of expression and association, online privacy, access to information, internet governance, cyber laws/policies, and cyber security. DRN is engaged in policy research and advocacy, public awareness campaigns, capacity building initiatives, and creating platforms to provide technical support, in collaboration with relevant stakeholders.

Out of The Box Media Literacy Initiative, Inc. is an educational nonprofit that creates innovative learning tools and experiences that foster media-literate Filipinos. It was awarded First Prize in the 2021 Global Media & Information Literacy Awards of the UNESCO MIL Alliance.

Hashtag Generation is an antiracist, feminist movement led and run by a group of young, tech-savvy Sri Lankans working towards building a society where everyone has the skills, information, and tools to be active participants in making the decisions that affect their communities, technologies, and bodies. Hashtag Generation mobilizes digital media tools to raise awareness and catalyze dialogue on important social justice issues.



Lead Writer

Shruti Trikanad, independent researcher

Research Oversight

Olga Kyryliuk, Technical Advisor on Internet Governance and Digital Rights, Internews

Sigi Mwanzia, Digital Rights Advisor, Internews

Vino Lucero, former Digital Rights Project Manager, EngageMedia

Prapasiri Suttisome, Project Officer, EngageMedia

Siti Rochmah Aga Desyana, Project Assistant, EngageMedia

Report Editor

Katerina Francisco, Editorial Coordinator, EngageMedia

Research Contributors

Bangladesh - Digitally Right

Cambodia - Cambodian Center for Independent Media

Indonesia - Southeast Asian Freedom of Expression Network

Maldives - Society for Peace and Democracy

Nepal - Digital Rights Nepal

Philippines - Out of The Box Media Literacy Initiative, Inc.

Sri Lanka - Hashtag Generation

Published August 2023



Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

ACKNOWLEDGEMENTS

We would like to express our gratitude to EngageMedia and Shruti Trikanad (Independent Researcher), who conducted this research and authored this report. Appreciation is also given to our Country Partners: Digitally Right (Bangladesh), Cambodian Center for Independent Media (Cambodia), Southeast Asian Freedom of Expression Network (Indonesia), Society for Peace and Democracy (Maldives), Digital Rights Nepal (Nepal), Hashtag Generation (Sri Lanka), and Out of The Box (Philippines), who provided meaningful insights for the research.

Shruti Trikanad is a Program Officer at the Centre for Internet and Society in India. Her research work focuses on digital identification systems, privacy, and data protection.

We are also grateful to all the communities and individuals who generously shared their time, experiences, and perspectives with us, and contributed to the research process.

This report is published under the USAID Greater Internet Freedom (GIF) project implemented by Internews and the GIF consortium.

This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of EngageMedia and do not necessarily reflect the views of USAID or the United States Government.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	7
REGIONAL OVERVIEW	12
COUNTRY REPORTS	26
BANGLADESH	27
CAMBODIA.....	38
INDONESIA.....	53
MALDIVES	64
NEPAL	77
THE PHILIPPINES	89
SRI LANKA.....	105



EXECUTIVE SUMMARY

This report focuses on the South and Southeast Asia (SSE Asia) region and is part of a multi-region research seeking to identify and compare the state of biometrics and digital identity threats, usage, and impact in Africa, the Balkans, Central Asia, Latin America and the Caribbean, and South and Southeast Asia.


This regional report by EngageMedia and Internews builds on seven country-level case studies that examined the implications of biometrics and digital identity (BDI) policies, systems, and practices in the SSE Asia region. The seven focus countries examined include **Bangladesh, Cambodia, Indonesia, Maldives, Nepal, Philippines, and Sri Lanka** (*focus countries*). The case studies addressed three research questions, namely:

1. What goal is the digital ID system meant to achieve, and is it succeeding?
2. What is the legal/policy framework surrounding the system, focusing on privacy, data sharing, surveillance, and exclusion?
3. What lessons can be learnt from existing knowledge on digital ID systems in developing countries?

BDI systems for identification purposes continue to be deployed at an accelerated rate in the SSE Asia region, due to their potential for enhancing service delivery, by both state and private entities, and improving citizen identification processes.¹ The case studies revealed that all seven SSE Asia countries are tapping into the BDI potential and:


- either have deployed a form of digitized identification system with biometric features (*Bangladesh, Cambodia, Indonesia, Maldives, Nepal, Sri Lanka*),
- have deployed a fully functional biometric digital ID system (*Philippines*),

¹ McKinsey Digital (2019). [Digital identification: A key to inclusive growth](#).

- 
- are currently transitioning and upgrading their existing identification or civil registration systems to a fully-fledged digital ID system (*Indonesia, Maldives, Nepal Sri Lanka*), or
 - are in the planning stages of digital ID adoption, as evidenced by national identification policy documents (*Cambodia*).

The case studies identified *one reality* and *four cross-cutting challenges* impacting all seven SSE Asia countries, to varying degrees. The *key reality* recognizes the pivotal role played by international development institutions, particularly the World Bank, and other South Asian countries, namely India, who are shaping the identification landscape in the seven SSE Asia countries. Collectively, the World Bank has provided financial assistance worth approximately USD 2.7 trillion to six out of the seven SSE Asian countries, in the form of either loans or grants, between 2011-2022, with the funds being actively disbursed between 2021-2022. The remaining country, Sri Lanka, has received a grant from the government of India, worth USD 3.8 million.

The *first challenge* is centered around countries' legal frameworks, namely their governing laws for identification systems, or their laws for the protection of privacy and personal data. Notably, identification systems that rely on biometric or other digital technologies must be underpinned by robust legal frameworks to ensure the protection of individuals' rights, and their personal data. It is also integral that these laws are aligned with international human rights standards and principles. By incorporating these elements, digital ID systems can foster trust, inclusivity, and transparency, while safeguarding individual rights. Concerningly, only three out of the seven SSE Asian countries (*Indonesia, Philippines, and Sri Lanka*) have enacted a stand-alone, unified, data protection legislation. This creates legal gaps in the BDI data collection ecosystem, with some countries permitting or engaging in excessive data collection.




The *second challenge* is centered around the opaque, ongoing collaboration between governments and third-party private entities, such as providers of BDI infrastructure or in-country private actors with access to BDI systems. Concerningly, there is limited transparency about these public-private partnerships, insufficient directives regarding third-party access to BDI systems for verification or authentication purposes, and limited information about data sharing agreements between states and private actors. The absence of well-defined policies and procedures related to transparency, accountability, and data disclosure could potentially compromise privacy and security.

The *third challenge* is centered on exclusion and discrimination arising from governments either mandating ID registration or mandating ID possession as a prerequisite for access to public or private sector services. The case studies found that some countries, namely Indonesia, Maldives, and Nepal, have transferred exclusionary practices observed in traditional ID methods to their digitized identification systems. The continued exclusion and discrimination prevent many vulnerable communities from obtaining a legal identity and gaining access to services that are dependent on such identity.

Illustratively, in Indonesia, representatives from the Ahmadiyah community filed a formal complaint against a local government in the West Java district, alleging that they were not being issued ID cards unless they renounced their faith. In Nepal, the Nepali ID system issues IDs only to Nepali citizens, therefore making proof of citizenship mandatory to obtain the ID. Women in Nepal are far less likely to hold citizenship documents than men, and differences are also seen among castes and religions, with persons from the Chepang and Musahar communities and Muslims lagging behind their peers in citizenship acquisition rates.


The *fourth challenge* is grounded in issues of affordability and accessibility to registration documentation (such as birth certificates) that are required to possess an



active and usable BDI, and ID registration centres. The existing digital gap shows that not all people are able to fully utilize the system due to geographical or funding constraints.

This regional report connects these findings to the broader regional context, contextualizing the distinct characteristics of the focus countries to identify common trends and approaches. This report highlights how the history of the region's restrictive regimes and limited understanding, representation, and contextualization of digital issues has influenced the current digitized identification infrastructure and legal frameworks. The regional report provides a series of recommendations for stakeholders involved in BDI systems at the design, implementation, and oversight levels.

- **For regional bodies:** to design guidelines and frameworks promoting best practices regarding the development and implementation of BDI systems. Specifically, develop guidelines for the appropriate, rights-respecting and accountable collection, use, and management of BDI data.
- **For local governments:** to provide rights-respecting provisions in their legal frameworks to ensure the protection of digital rights, the alleviation of exclusion and discrimination impacting vulnerable or excluded communities, the enhancement of data protection, and the provision of grievance, redressal, and oversight mechanisms.
- **For civil society:** to advocate for rights-respecting safeguards for the management and utilization of digital ID and biometric data. Further, advocate for alternative forms of identity proof, to avoid creating an unnecessary dependence on one form of identity credential.



As digital identification systems continue to evolve, it is essential to strike an appropriate balance between technological advancements, efficient service delivery, individuals' privacy protections, and the promotion of digital rights.



REGIONAL OVERVIEW

Introduction

The World Bank defines ‘digital identity’ as a ‘set of electronically captured and stored attributes and/or credentials that uniquely identify a person.’² Biometric identification refers to ‘the process of searching against a biometric enrollment database to find and return the biometric reference identifier(s) attributable to a single individual,’ with biometric identification systems serving this purpose.³

The UN Sustainable Development Goal 16.9 promotes legal identity for all by 2030, and among efforts to reach this goal is the development and implementation of biometrics and digital identity (BDI) systems across the globe. BDI systems are touted to be improvements from their manual, paper-based identification predecessors, due to their heightened security and convenience, as they “cannot be borrowed, stolen, forgotten, or forged.”⁴ Currently, at least 100 countries have collected their citizens’ biometric data for some sort of an identification system, ranging from national ID cards to passports,⁵ with more planning to do so in the near future.


Notwithstanding these benefits, this regional report affirms that the rising implementation of BDI systems in the seven South and Southeast Asian countries explored under the GIF project raises human rights concerns for individuals and communities. As these national ID systems with biometric features are increasingly being intended to facilitate access to many public and private services, marginalized and vulnerable groups who do not have legal forms of identification are denied access

² The World Bank. [Practitioner’s Guide: Glossary](#).

³ International Organization for Standardization (2022). [ISO/IEC 2382-37 \(2022\)](#).

⁴ Kelsey Atherton (2022). [The enduring risks posed by biometric identification systems.](#)

⁵ Paul Bischoff (2022). [Biometric data: 100 countries ranked by how they’re collecting it and what they’re doing with it.](#)



to critical services, exacerbating their continued exclusion and marginalization. These services range from access to health care and participating in elections to applying for bank accounts and registering civil events.


Further, the collection of vast amounts of personal data in digital identification systems poses a considerable threat to people's privacy and the protection of their personal data, where proper safeguarding measures are not adopted prior to deployment. These measures range from policy and legal instruments, such as internalizing and ensuring adherence to the principles of data protection, including purpose limitation and data minimization, to conducting human rights impact assessments to mitigate risks to users and technological innovations, such as the use of encryption to protect personal data, amongst others.

In the South and Southeast Asian context, the COVID-19 pandemic played a role, in part, in the increase of digital users, given the imposition of limitations on physical movement and physical interactions in public spaces such as schools, work environments and buildings, and hospitals. However, the issue of the digital divide still looms over the SSE Asia region; 31% of the total population – or roughly 150 million adult individuals – are digitally excluded for various reasons, including challenging geographic constraints and uneven distribution of economic activities.⁶ In South Asia, about a billion people – mostly coming from remote areas – are still not connected to the internet, and smartphones remain unaffordable for millions of people.⁷

Further, concerns relating to data privacy and protection are also present. ID data is arguably the most personally identifiable and, where biometrics are collected, sensitive data available on individuals, permitting privacy violations *at scale* where

⁶ Roland Berger (2021). [Bridging the digital divide: improving digital inclusion in Southeast Asia](#).

⁷ Hartwig Schafer & Christine Zhenwei Qiang (2022). [Towards a Thriving Digital Economy in South Asia](#).



this is accessed by unauthorized persons. This is contextualized against reports of citizens' personal identification data being leaked in several SSE Asian countries, such as Philippines⁸ and Bangladesh⁹ due to a combination of weak security systems and inadequate laws to secure data protection and promote data privacy that is managed by government entities. Existing digital ID infrastructure and cybersecurity measures in some SSE Asian countries are deemed insufficient to properly protect individuals' data under the government's care. Illustratively, following recurrent data breaches in Indonesia, hackers described the country's cybersecurity system as 'really awful' due to the poor quality of the country's data protection and cybersecurity measures.¹⁰ During these breaches on government databases, hackers claimed to have illegally obtained "ID card photos, family card pictures, tax IDs", amongst others.¹¹ With the Indonesian government's planned transition towards a digital ID system that collects personal (demographic) and sensitive personal (biometric) data, this data breach issue will likely be amplified to a higher degree, posing greater privacy risks for Indonesians.


This report stresses that BDI design and deployment in the SSE Asian region be examined and pursued from a well-informed contextual lens, noting the regions' diverse historical and socio-political landscape, characterized by various governance systems, and diverse cultural, religious, economic and technological contexts. In some instances, periods of authoritarian rule and regimes may have created gaps in the personal information protection ecosystem, where the protection of citizens' data was not prioritized or neglected.

⁸ Davinci Maru (2023). [Over 1.2M records from NBI, PNP, other agencies leaked, firm says.](#)

⁹ Lorenzo Franceschi-Bicchierai (2023). [Bangladesh government website leaks citizens' personal data.](#)

¹⁰ The Jakarta Post (2022). [Hackers: 'I think Indonesia's cybersecurity is run by 14-year olds.](#)

¹¹ *Ibid*



Building on this, in the 2020s, expanding surveillance projects and targeted attacks towards government critics, human rights defenders and activists, and the general public have been documented across nearly all seven focus countries.¹² Illustratively, the Government of the Philippines adopts ‘red-tagging’ practices that label a particular individual, often government critics, with association to communism and/or terrorism. This usually leads to the publication of the accused individual’s personal data, specifically their full names, on an official government website which further endangers suspected individuals.¹³

Despite this, the region has also witnessed significant progress in recent years towards strengthening the protection of personal data through the enactment of data protection and privacy frameworks. Many SSE Asian countries have recognized the importance of safeguarding citizen data and have taken steps to develop legal frameworks, enact privacy laws, and establish regulatory bodies to address historical challenges and strengthen data protection mechanisms to ensure the responsible use of citizen data. Indonesia, for example, has recently passed the Personal Data Protection Act in 2022, which emphasizes the accountability of all entities hosting and managing public identification data. Consent rights for data subjects have also been included into the draft Bangladeshi Data Protection Act (2023).

To understand the current digital ID landscape in the SSE Asia region, EngageMedia in collaboration with Internews undertook research on ***The State of Digital Identification Systems in South and Southeast Asia***. By analyzing the key emerging trends in the implementation of biometric and digital identification systems, highlighting the SSE Asia region's diverse approaches and shared challenges, this

¹² The Carnegie Endowment for International Peace (2021 - 2023). [Politics of Opposition in South Asia](#); Chatham House (2021). [Freedom of expression under threat in Southeast Asia](#).

¹³ Kristine Joy-Patag (2020). [‘Mother of red-tagging’: No process yet to remove names from terror list](#).


research analyzes the implications on digital rights, and proposes actionable recommendations to relevant stakeholders to address attendant challenges.

Methodology

Table 1: Research Topic and Research Question (by EngageMedia)

Research Topic	A Comparative Analysis on Biometrics and Digital Identification System Trends in SSE Asia Countries
Research Questions	<ol style="list-style-type: none"> 1. What are the prevailing trends and common approaches in biometrics and digital identity systems across seven focus countries? 2. How do these trends vary across the focus countries, and what are the underlying factors contributing to these differences? 3. How do the existing digital ID policies and frameworks in SSEA impact inclusion and exclusion, particularly concerning marginalized and vulnerable groups? 4. Based on the analysis of the regional trends, what policy recommendations can be proposed to relevant stakeholders to create more inclusive and equitable digital identity systems in seven focus countries?

This regional report functions as a summary and an overview regarding existing trends on biometrics and digital identity in seven focus countries, and provides a contextual synthesis by linking these trends to issues in the region. It uses qualitative methods by examining the results of all seven country reports and integrating it into a more nuanced regional narrative that extricates similar themes and trends across the focus countries. It relies primarily on secondary sources as presented by the



country research, interpreting and analyzing the findings to draw regional conclusions for the matter.

Research Limitations

This research report was limited by the following:

- **Assumptions in sources:** this report relied on publicly accessible material, with the reviewed studies and reports containing the assumptions of respective authors in their individual and professional capacities.


Regional Findings

The following key emerging issues and trends were identified, namely, the inadequate laws for existing BDI infrastructure, the non-transparent collaboration between states and third-party actors, and the harms of exclusion and discrimination to vulnerable groups.

1. Inadequate Laws for Existing Digital ID Infrastructure

Identification systems that rely on biometric or other digital technologies must be underpinned by robust legal frameworks to ensure the protection of individuals' rights, and their personal data. It is also integral that these laws are aligned with international human rights standards and principles. By incorporating these elements, BDI systems can foster trust, inclusivity, and transparency, while safeguarding individual rights.

Internationally, standards regarding the collection, management, and interoperability of biometric data have been continuously developed and updated in line with technological advancements. For example, the International Organization for Standardization has issued various standards related to the collection of biometric




data in a rights-respecting and accountable manner, that local governments and regional bodies can customize and incorporate into their domestic laws.¹⁴

Across the region, a concerning, prevailing trend that was observed is the failure to deploy BDI systems, in their varying formats, with the enactment of comprehensive personal data protection laws or comprehensive governing laws for identification systems. Concerningly, some of the established legal frameworks lack clearly-defined provisions to properly collect and store personal and sensitive data, in a transparent and accountable manner. The main issues noted in many of the existing policies and regulations were centered around the collection and management of people's biometric data, accountability systems, and grievance redress systems.

Out of the seven SSE Asian countries, only three (*Indonesia, Philippines, and Sri Lanka*) have enacted a stand-alone, unified, data protection legislation. Out of these three countries, two are still in the nascent stages of implementing and operationalizing their laws (*Indonesia and Sri Lanka*). The remaining four countries either do not have a unified, comprehensive data protection law, or are in the drafting stages of their law. This creates legal gaps in the BDI data collection ecosystem, with some countries permitting or engaging in excessive and unnecessary data collection practices.

In terms of data management, the main issues observed included the vague description of what data is being collected, who has access to the data, and how long the data is stored in the ID database or system. For example, Nepal's new Identity Act (2020) details broad access rights to the existing National ID Card Management database for all government agencies and 'some private services', but fails to detail the latter entities. Further, by virtue of the linkage between the ID and civil registration

¹⁴ This does not amount to an endorsement of these standards. See: The International Organization for Standardization - ANSI (2002). [ISO/IEC JTC 1/SC 37 on Biometrics](#); The International Organization for Standardization and the International Electrotechnical Commission (2019). [ISO/IEC 39794-1:2019\(en\)](#).




datasets, Nepal also permits the collection of a vast amount of information and the indefinite storage of all data in an electronic database about every Nepali citizen in a manner that falls short of the data minimization principle.

Bangladesh, in its Data Protection Act (2023) broadly exempts penalties for access to digital data for ‘law and order purposes.’ Its governing law for identification permits the collection of Deoxyribonucleic Acid (DNA) data that is excessive, unnecessary, and dangerous. The collection of DNA data was found to be excessive by the High Court of Kenya.¹⁵

Similarly, the case studies documented cross-cutting challenges in the governing laws establishing identification systems. While countries such as the Philippines have positively provided for the expansion or reduction of national ID data points (i.e., the *collection of personal or demographic data*) as a legislative, rather than an executive function, this has not been replicated across the other countries. Illustratively, Sri Lanka’s Registration of Persons Act (RPA), as amended most recently in 2016, delegates the responsibility of prescribing the data that will be collected and stored in the national registry to the executive government through regulations. While this is common in other digital ID systems around the world, it is still a concerning practice, because it permits the addition of new categories of data to be collected without undergoing the legislative process.

Broad provisions like these open the possibility of expanded state power, as they leave the door open for governments to demand additional data collection requirements and access to sensitive data without sufficient checks and oversight. This trend magnifies the need for governments to prioritize the development and

¹⁵ *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR.



implementation of robust legislation and policies to safeguard citizen data and ensure accountability, with support from regional bodies.


Related to privacy concerns are issues of state-facilitated surveillance, which is closely related to fears around the collection of massive datasets for purposes of deploying digital ID systems. Across the region, and as explored above, legal frameworks and policies currently fail to specify which actors have access to data and for which purposes.

This failure directly impacts data subjects and ID users' right to request for data erasure. In the case of the Philippines, the current governing law does not expressly provide ID holders with the right to delete their data records, which is a notable concern given the vast purposes of the biometric ID and the potential for surveilling a user's day-to-day life.

2. Non-Transparent Collaboration between States and Third-Party Actors

The opaque, ongoing collaboration between governments and third-party private entities, such as providers of BDI infrastructure or in-country private actors with access to BDI systems is an important trend observed in the region. These public-private partnerships raise concerns about the limits imposed on corporations' access to individuals personal and sensitive data. This impacts data privacy and security, as in many cases, information on who has access to the data, for how long, and for what purposes are not clearly spelled out in existing disclosures.

This report notes that third-party cooperation, as a minimum, would be ideal when there is a clear, definitive legal basis on a collaboration or partnership with the state. Further, there should be clear transparency and accountability mechanisms in place to promote public scrutiny and oversight. However, the case studies documented a different, and concerning trend.



Concerningly, there is limited transparency about these public-private partnerships, insufficient directives regarding third-party access to BDI systems for verification or authentication purposes, and limited information about data sharing agreements between states and private actors. For example, in the Maldives, the government has collaborated with a third-party, private infrastructure provider registered in England, SumSub Ltd, to store citizens' biometric face recognition data captured in the Maldives' digital ID system, the eFaas. Problematically, provisions delineating each entity' obligations and the specific details of the data storage and safeguard measures are canvassed under a private contract. It is unclear whether this contract is subject to an accountability mechanism, and what law, regulation or policy governs the contract.


Similarly, Cambodia's upcoming facial recognition project in collaboration with Local Conglomerate HSC Group has also come under scrutiny. This is due to the fact that HSC Group has been involved in various government identification and surveillance projects, such as running the current system for national ID cards, printing passports and providing border checkpoint technology.¹⁶

The absence of well-defined policies, procedures and agreements related to transparency, accountability, and data disclosure and data sharing could potentially compromise ID users' data protection, privacy, and the safety and security of data in ID databases. In turn, this prevents a full, independent human rights risk assessment or an audit.

3. Exclusionary Practices

Ideally, digital ID systems are designed to address two main problems. The first includes the provision of a form of identification that would allow users to be digitally

¹⁶ Fiona Kelliher (2023). [Cambodian Facial Recognition Effort Raises Fears of Misuse](#).



verified when accessing public and private services provided within online platforms. The second is to bridge the gap caused by the existing traditional identification system that may be exclusionary for some.¹⁷

However, this research finds that existing exclusionary practices for obtaining traditional identification documents are carried over to the proposed or established BDI system of many SSE Asian countries. Many individuals who face difficulties in accessing traditional ID documentation and systems are also unable to obtain digital IDs, further marginalizing them and limiting their access to subsequent services. Further, governments are either mandating ID registration or mandating ID possession as a prerequisite for access to public or private sector services.

In Cambodia, registration for national IDs is reliant on birth certificates, excluding minority communities (such as Vietnamese residents living in Cambodia).¹⁸ In Nepal, IDs are accessible to those with citizenship documents, but the possession of such documents is associated with gender, caste, and intra-family dynamics at the household level. Other examples include Indonesia's exclusion of certain faith groups, such as Ahmadiyah and indigenous faiths,¹⁹ and the gender bias in birth registration in the Maldives, which translates into inability for some communities to access Digital ID and its subsequent services.

This continued exclusion and discrimination prevents many vulnerable communities from obtaining a legal identity, and gaining access to services that are dependent on such identity. Governments in the SSE Asia region should prioritize inclusive policies that address these exclusionary practices, ensuring that all citizens can access their rights and services.

¹⁷ *Ibid*, n.1

¹⁸ Try Thaney (2022). [Khmer Krom in Cambodia still face challenges getting ID cards.](#)

¹⁹ King Eben Lumbanrau (2023). [Ramadan hopes of Ahmadis in Lombok who have been displaced for dozens of years – "Home is heaven on earth."](#)



Recommendations


As digital identification systems continue to evolve, it is essential to strike a balance between technological advancements, privacy protections, and the promotion of digital rights. This regional synthesis, and the accompanying seven country case studies, seek to contribute to the ongoing biometrics and digital ID discourse and provide valuable insights for policymakers and stakeholders working towards the development of fair, inclusive, and human-centric digital identification systems in South and Southeast Asia.

Overall, the two core issues of data protection and privacy and exclusionary practices must be addressed by the identified stakeholders to ensure the proper implementation of a rights-respecting and inclusive identification system. Based on this, the report proposes the following recommendations to SSE Asian stakeholders, namely regional bodies, local governments and civil society actors.

Regional Bodies

We urge regional bodies with human rights, ICT and other rights-related mandates in the SSE Asia region, such as the Association of Southeast Asian Nations (ASEAN), to:

- Design guidelines and frameworks promoting best practices regarding the development and implementation of BDI systems. Specifically, develop guidelines for the appropriate, rights-respecting and accountable collection, use, and management of BDI data.
 - Cognizant of the need for contextualized data protection and biometric data approaches at the regional level, we recommend the ASEAN draws inspiration from the European Union's General Data Protection



Regulation (GDPR) and the ISO/IEC 39794 (2020) international standard regarding biometric data management.

Local Governments


We urge local governments in the SSE Asia region to:

- Provide rights-respecting provisions in their legal frameworks to ensure the protection of digital rights, the alleviation of exclusion and discrimination impacting vulnerable or excluded communities, the enhancement of data protection, and the provision of grievance, redressal, and oversight mechanisms. Specifically, these frameworks should:
 - Satisfy the three-part test under Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR)
 - Create accountability and grievance redress mechanisms to ensure proper oversight over entities collecting identification data, a clear delineation of relevant parties' responsibilities, and provide individuals with mechanisms for filing and resolving ID-related complaints.
 - Create mechanisms to ensure transparency and protect citizen data from unauthorized access or misuse, such as properly equipped data protection authorities.
 - Allow other forms of alternative identification in digital ID systems to end the continued exclusion and marginalization of vulnerable groups.

Civil Society

We urge civil society actors in the SSE Asia region to:

- Advocate for rights-respecting safeguards for the management and utilization of digital ID and biometric data.

- 
- Advocate for alternative forms of identity proof, to avoid creating an unnecessary dependence on one form of identity credential.

COUNTRY REPORTS



DIGITAL ID IN BANGLADESH

Summary

The People's Republic of Bangladesh (or Bangladesh) has deployed a foundational identity (ID) system with biometric features with support from the World Bank and the United Nations Development Programme. The foundational ID system has been continuously strengthened over the years but a number of significant shortcomings remain.

Notably, universal coverage has not been achieved, and there is no comprehensive governing legal framework. This case study recommends that the law governing national identification systems be amended to include all significant facets of the ID system, including the rights and obligations of data subjects and administrators, grievance redressal procedures, and rules for governing bodies and potential private actors.

Moreover, to ensure that citizens are fully informed and empowered and to hold responsible parties accountable for any ID-related harm, the system should not be made mandatory for accessing services until universal coverage is accomplished.

Historical Context

Bangladesh's digital economy and transformation programme, 'Digital Bangladesh', has had different goals since it was first announced in 2008, and launched in 2009.¹ Despite this, 'Digital Bangladesh' is underpinned by one overall vision: for Bangladesh to undergo a digital transformation.² To this end, the government began implementing a series of digital policies to create the infrastructure for deploying reliable public services. A key element of this agenda was the promotion of efficient electronic services (or e-services) through the development of a National Identification (NID) system as a foundational ID system. This system was intended to aid in effective public policy formulation by offering citizen identification and verification for various public and private service deliveries.³ The core information available through the system would help track a wide range of transactions undertaken by the public sector – from the collection of tax revenue to the delivery of social benefits – and systematize a wide range of record-keeping, from land cadasters⁴ to utility connections.

Bangladesh's existing identification system originated from the preparation of an electoral voter list database of 87 million citizens for the ninth parliament election in 2008. In addition to creating a comprehensive database of voters, it also created a widespread demand for an ID card scheme in the country.⁵ The Bangladesh Election Commission (BEC) created the electoral rolls, and this process brought about greater


¹ Prime Minister's Office, Access to Information Programme (2009). [Digital Bangladesh Concept Note](#).

² The Daily Star (2023). [Digital Bangladesh: A story of transformation, resilience and sustainability](#).

³ World Bank (2011). [BD Identification System for Enhancing Access to Services \(IDEA\) Project: Project Appraisal Document - Appraisal Stage](#).

⁴ This refers to "an official record of the owners of land and of the amount and value of the land they own, used for calculating the amount of tax owed." Cambridge Dictionary. [Cadastré](#).

⁵ Government of the People's Republic of Bangladesh and the United Nations Development Programme (2007). [Project Document: Preparation of Electoral Roll with Photographs](#).



transparency and reliability in the identification of voters. With the support of donors and the UNDP, other building blocks preparing the country for the foundation ID system were also implemented: a database comprising 87 million voters (citizens aged 18 and above) with biometric information; experience with the issuance and updating of a voter ID card; and capacity building with the Bangladeshi service industry.⁶

Building on this voter database, the BEC created the National Identification System (NIS), which required citizens to submit their biometric information leading to the issuance of national ID cards. This is a smart ID card containing an embedded microchip and featuring a unique 10-digit identification number – the National Identification Number (NIN). The ID card is used to access a wide variety of public and private services, including banking account opening services, mobile SIM registration, voter registration, amongst others.⁷


Involvement of the World Bank

In May 2011, the World Bank approved a USD195 million concessional credit project, the ‘Identification for Enhanced Access to Services (IDEAS) Project,’ to assist the Government of Bangladesh in developing a reliable and accurate national identification system. The proposed objective of this project was to *“support the Government in issuing ID cards with robust security features, developing capacity to provide identity verification services, and developing capacity over the longer term to begin to integrate the new ID system into a wide range of both public and private services.”*⁸

⁶ Government of the People’s Republic of Bangladesh and the United Nations Development Programme (2007). [Project Document: Preparation of Electoral Roll with Photographs](#).

⁷ Mohammad Rashed and ASM Ahsan Habib (2021). [How to build e-NID with existing IDs in Bangladesh](#).

⁸ World Bank (2011). [World Bank Supports Digital Bangladesh through National Identification System](#).



Critically, the project aimed to issue identification numbers and cards to about 90 million Bangladeshi citizens of age 18 and above in five years, to enable the efficient and transparent delivery of benefits and service to citizens, particularly the poor.⁹

The first component of the project involved establishing a regulatory and policy framework for the NID and its integration into service delivery.¹⁰ At the time, the only governance framework for the ID system was the National ID and Registration Act, 2010 (later renamed the National Identity Registration Act, 2010). This Act provided a high-level framework for the Bangladesh Election Commission (BEC) by establishing an independent National ID Wing and tasking it with the maintenance of the national identification system.¹¹


However, it did not have any regulations concerning the *actual operation* of the NID system – including issues of privacy, access to information by public and private actors, security measures to protect the information, limitations to the use of the data, amongst others. Since the NID system was also meant to be linked to various public services, it was crucial to have a published policy on how the system may be used, and what controls are in place to prevent misuse or breach of the system.

The project was set to provide technical assistance to the BEC and other relevant agencies in drafting regulations to address potential issues that accompany the operation of a national ID system, along with capacity building and technical assistance to help integrate the system into service delivery platforms. Key among these was creating and supporting identity verification services, along with integrating them into the country's existing civil registration systems, largely digital

⁹ *Ibid.*

¹⁰ *Ibid.*, n. 2

¹¹ Legislative and Parliamentary Affairs Division, Ministry of Law, Justice and Parliamentary Affairs. [National Identity Registration Act, 2010](#).



birth and death registration systems. This would have ensured easier onboarding of citizens, with fewer errors and exclusions.¹²

Another objective of the project was to support the design and deployment of technology infrastructure and facilities for the NID, including a data center and disaster recovery site, a data communications network, a decentralized technology infrastructure, the enhancement of database contents, and the production, personalisation, and delivery of NID smart cards to citizens.¹³

The World Bank project was completed in 2018, with only moderate results. There were significant delays in the implementation of NID laws and regulations, and they were only able to issue half the number of targeted NID cards.¹⁴

Identification System: Legal Framework

National Registration Act, 2010

In 2010, the National Identity Registration Act (or NIR Act, 2010) was enacted and provided the legal framework for the NIS. The original voter ID was renamed National Identity Number (NID) through Section 2(3) of NIR Act, 2010. In 2013, the National Identity Registration (Amendment) Act was passed, which introduced measures addressing the creation of an ID database and allowing the verification of citizens' identities. The NIR Act (2010) designates a part of the BEC, the National ID and Registration Wing (NIRW), as the administrator of the NID System.


Proposed National Identity Registration Act, 2022

In June 2023, the Cabinet approved the draft National Identification Registration Act, 2023. The proposed law will change the supervision of the NID registration and operation

¹² *Ibid*, n.3.

¹³ World Bank (2018). Implementation [Completion Report Review, BD: IDEA project](#).

¹⁴ *Ibid*, pp. 10.



from the BEC to the proposed NID Registrar's Office under the Ministry of Home Affairs, Security Services Division. The draft act also proposes the introduction of a unique ID number for citizens, issued during birth registration.¹⁵ As of July 2023, the draft law is pending approval by Parliament, and if obtained, this will trigger changes in Bangladesh's foundation ID systems and processes.

Implications of Bangladesh's ID system

Eligibility for NID

Initially, according to the NIR Act (2010), only citizens who are listed as voters under the Electoral Rolls Act were eligible for a national ID card.¹⁶ However, the NIR Amendment Act (2013) added a provision allowing the Commission to issue cards to non-voters, subject to prescribed rules.¹⁷ The NIR Act (2010) does not make it mandatory for citizens to register for a NID and does not ascribe any punishment for non-registration. However, the NIR Act (2010) requires individuals to present their national identity card when accessing certain services or facilities. However, the requirement will not be implemented or enforced until all citizens in Bangladesh receive their national identity cards and a gazetted notice is issued by the government.¹⁸ This requirement is further restricted by the provision that a citizen cannot be deprived of their rights or civil benefits for not having the national ID card.¹⁹ This is an important safeguard and can be a crucial step in precluding incidents of exclusion.


¹⁵ Media New Age (2023). [Home Ministry to get NID Job from EC.](#)

¹⁶ Section 5, National Identity Registration Act, 2010.

¹⁷ Section 2, [National Identity Registration \(Amendment\) Act, 2013.](#)

¹⁸ Section 11, National Identity Registration Act, 2010.

¹⁹ *Ibid.*



The experience of India with Aadhaar showed that because such a safeguard in the law came as an afterthought, many years after the use of Aadhaar had become *de facto* mandatory in the country, it was not able to achieve much in preventing its exclusionary impact.²⁰ Although the impact remains to be seen in Bangladesh, it is hoped that the inclusion of the provision before the transition to a fully-fledged digital ID system is finalized will make it more effective.

Data Collection and Storage

Since the NID is based on the voter ID database, most of the data stored in the NID registry is taken from the former. The Act does not specify what demographic or personally identifiable information is collected from citizens during ID registration, while providing a broad definition of data as “*data collected during the composition, amendment or updating of voter list intended for the National Identity Registration as per the Electoral Rolls Act 2009.*”²¹

The NIR Act (2010) permits the collection of biometric information, which is defined to include the following features: (1) fingerprint, (2) hand geometry, (3) palm print, (4) iris, (5) facial recognition, (6) DNA (Deoxyribonucleic Acid), (7) signature, and (8) voice.²² These categories of biometric data that may be collected under the Act are excessive, unnecessary, and dangerous.


Some of these data points – most notably DNA – have been extensively debated in other countries and held unconstitutional for their unjustifiable risks to privacy and discrimination.²³ Even if such data is not currently being collected or used, its legislative inclusion means that it can be legally collected by the government by simply issuing notifications or regulations, without further debate. This is dangerous

²⁰ Ananya Bhattacharya and Nupur Anand (2018). [Aadhaar Is Voluntary – but Millions of Indians are Already Trapped](#).

²¹ Section 2(4), National Identity Registration Act, 2010.

²² Section 2(8), National Identity Registration Act, 2010.

²³ [Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.](#) [2020] eKLR.



and allows for greater risks in the national ID system than is necessary to achieve its purposes.

Data Protection

Although the NIR Act (2010) is the governing law for the issuance of the national ID card and the management of the ID database, it does not regulate most aspects of the ID system, leading to the conclusion that the law is not comprehensive for purposes of ID management. This recognition underpins the development of the draft National Identification Registration Bill, 2023.


Illustratively, the current law identifies the BEC as the administrator of the national ID program, charged with identity registration, the issuance of NIDs, and all other responsibilities related to the ID program. However, it fails to detail the rights or duties of citizens, the access that actors have to the system, the system's security, or even the various uses of the system.

In relation to the protection of data collected through the ID system, the NIR Act (2010) simply provides that the database will be considered a “confidential” database which can be accessed if a person or institution applies to the commission for certain data; the commission shall share such data unless it considers otherwise.²⁴ The Act also prescribes punishments for the tampering of data in the ID program, and negligence of duties by persons or government employees or officers.²⁵

On March 14, 2023, the Information and Communications Technology Division of the Ministry of Posts, Telecommunication, and Information Technology published the proposed Data Protection Act, 2023 (or draft DPA, 2023). The Bill is loosely based on the European Union's Data Protection Regulation (Regulation (EU) 2016/679), having concepts of data controllers, data use limitation principle, access and withdrawal of

²⁴ Section 5, National Identity Registration (Amendment) Act, 2013, as amending Section 13 of the 2010 Act.

²⁵ Sections 16a and 17a, National Identity Registration Act, 2010.



consent rights for data subjects, data erasure, amongst others, that are critical to ID data protection and security.²⁶

However, the draft DPA (2023) has been met with a lot of criticism over several features that allegedly raise serious privacy concerns with a direct impact on Bangladeshi citizens.²⁷ The concerns that are largely relevant to the national ID database include:


1. Failure to Define Personal Data or Personally Identifiable Data: The draft DPA 2023 only provides a definition of sensitive data, without distinguishing personal data or personally identifiable data. The failure to contextually categorize different types of data can impact the ID database administrator's classification of different types of data and their sensitivity levels. Notably, classifying all data as 'sensitive data' mandates entities to adopt more stringent data protection measures given the risk to data subjects' human rights.²⁸
2. Exemptions Granted for Law-and-Order Purposes: Broad exemptions, including “for the prevention or detection of crime or for the purpose of investigations; or the apprehension or prosecution of offenders; or the assessment or collection of any tax or duty or any other imposition of a similar nature” are provided under the draft DPA (2023).²⁹ If this provision is passed as it is, it may allow unfettered access to significant personal data collected in the national ID database, without any judicial controls or oversight, or without the requirement to provide justification for this data access. Since the NIR Act

²⁶ EUR-Lex (2016). [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC \(General Data Protection Regulation\)](#).

²⁷ The Daily Star (2023). [Why the Draft Data Protection Act is Concerning](#); Amnesty International (2023). [Bangladesh: New Data Protection Bill threatens people's right to privacy](#).

²⁸ Atlantic Council (2023). [Bangladesh draft data protection act 2023: Potential and pitfalls](#).

²⁹ Section 33, draft [Data Protection Act 2023](#).



(2010) also does not create any obstacles in accessing this information, it poses grave risks for misuse by government actors. At the very least, this exemption should be allowed only on the basis of a judicial order.

3. Lack of Independence of the Data Protection Authority: The proposed data protection authority under the draft DPA (2023) is the Digital Security Agency (DSA). The DSA is a government security and intelligence agency that was established under the Digital Security Act, 2018.³⁰ The proposed data protection authority will be headed by the Director General of the DSA, and four directors appointed by the government. The independence of this agency is questionable for two reasons, namely (1) the DSA is a state entity with monitoring and surveillance capabilities, that is in the direct control of the government, and (2) the government acts as the data controller of ID data, and the appointment of a non-independent state entity to oversee compliance with the law amounts to a major conflict of interest.

Conclusion and Recommendations

The Bangladesh foundational ID system has been in a continuous state of development and changes since it first began in 2008, including with interventions from the World Bank and the UNDP. Despite this, the system is still lacking in many crucial ways, including having a comprehensive governing, legal framework or achieving universal coverage.

³⁰ *Ibid*, Section 35.



Recommendations

We urge legislators in Bangladesh to:


- Ensure that the draft National Identification Registration Bill, 2023 covers all the important aspects of the ID system and adheres to international best practices.

This includes:

- Detailing (a) the actors that may in any way interact with the system, (b) grievance redress mechanisms, (c) the rights and duties of data subjects and the administrator of the system, amongst others.
- Detailing how and whether government actors (and private actors, if allowed) can use the ID database, and mandate that these actors detail their use of this data through publicly available policies, limited to the permissible purposes. In the absence of this, citizens are not well equipped with knowledge of what they can expect under the system and do not have the resources to hold anyone accountable for any harm caused through the use of the ID.

We urge the ID administrator, currently the BEC, and shortly the proposed NID Registrar's Office under the Ministry of Home Affairs, Security Services Division, to:

- Refrain from triggering the provision under Section 11 of the NIR Act, 2010 making the NID compulsory to access services or facilities, especially where universal coverage has not been achieved.



DIGITAL ID POLICIES AND PRACTICES IN CAMBODIA

Summary

The Kingdom of Cambodia's (or Cambodia) ranks 127th out of 193 countries in the UN E-Government Development Index, demonstrating a positive drive towards digital transformation.¹ However, Cambodia has fallen in the press freedom rank, from 142/180 to 147/180, given that “governmental persecution of independent media has intensified in the run-up to elections” scheduled for 23 July 2023.² This operating environment, where press freedom is limited, affects the public availability of information on government policies and processes. This case study is impacted by limited information about Cambodia's planned digital identity (ID) system.

Despite this, from the material examined below, it is evident that the country needs to address the risks of discrimination and exclusion that digital ID systems introduce, particularly for migrants from neighbouring states. To ensure maximum participation and limit discrimination.

¹ UN E-Government Knowledgebase (2022). [Cambodia](#).

² Reporters Without Borders (2023). [Asia-Pacific: Cambodia](#).

- The National Social Protection Identity (NSPI) should separate nationality and citizenship records from the digital ID and authentication platform, providing alternative ways for individuals to obtain a Khmer ID and participate in the Integrated Population Identification System (IPIS) platforms.
- Special measures should be implemented to accommodate individuals without government identification records and allow alternative proof of identity (ID) documents for access to the IPIS, similar to the Indian Aadhaar system.

Historical Context and Background

Over the past decade, Cambodia has sought to advance further towards digital transformation and transition towards a digital economy. Internet penetration stood at 60% of the total population in 2021,³ and more Cambodians are relying on online platforms for news and information. However, digital spaces and technology are also increasingly becoming tools for political control, and Cambodian citizens face growing threats to their privacy and data security online.

According to Freedom House, Cambodia is rated 'not free',⁴ with the government of Prime Minister Hun Sen cracking down on the opposition and the independent press. Further, several decades of migration from neighbouring states, combined with limited or destroyed legal records, have resulted in several communities not having government identity documents.

³ The World Bank (2020). [Individuals using the Internet \(% of population\) - Cambodia](#).

⁴ Freedom House (2023). [Freedom in the World - Cambodia](#).

Civil Registration System

The Kingdom of Cambodia's modern Civil Registration and Vital Statistics (CRVS) system is a national system to register births, deaths, and marriages within its jurisdiction. The process started in 2002 but recorded less than 5% or 300,000 people of the 13 million population registered up until 2004.⁵ The Ministry of Interior's nationwide mobile civil registration campaign in 2004 changed this, resulting in a birth registration rate of over 90% by December 2006.⁶

The CRVS system is largely managed by the General Department of Identification (GDI) of the Ministry of Interior and involves the Department of Civil Registration, the Department of Administration, the Department of Population Statistics, the Department of Identification Cards, the Department of Passports, and the Department of Information Systems.⁷

Generally, a legal basis for a CRVS system is important in establishing an identification system, as it defines the legitimate purpose and limitations of the system. Promisingly, Cambodia adopted the Civil Registration, Vital Statistics, and Identity (CRVSID) law on June 21, 2023, with the law scheduled to take effect after 12 months. According to the Global Health Advocacy Incubator,


“This comprehensive legal framework establishes an integrated system which links the civil registration of births and death, along with individuals’ identification and residence, to a newly created population register. The law also removes obstacles and disincentives from the registration process, establishes a universal right to an identity (ID) card for all citizens and includes important privacy protections for personal data.”⁸

⁵ Centre of Excellence for CRVS Systems (2020). [Snapshot of Civil Registration and Vital Statistics Systems of Cambodia](#).

⁶ *Ibid.*

⁷ General Department of Identification/Ministry of Interior (2016). [National Baseline on Civil Registration and Vital Statistics in Cambodia](#).

⁸ Global Health Advocacy Incubator (2023). [Cambodia's Newly Adopted Law Guarantees Universal Legal Identity and Complete Registration of Births and Deaths for All](#).



Prior to this law taking effect, the following laws will continue to govern Cambodia’s civil registration system: (1) Law on Marriage and Family (1989), (2) Law on Nationality (1996), (3) Sub-decree No. 103 on Civil Registration (2000), and (4) Civil Code (2007). This system was largely paper-based, and digitisation efforts began in 2017 with the National Strategic Plan for Identification (NSPI) 2017 - 2026, which is explored in more detail below.⁹

Current Identification Systems

Khmer National ID

The “Khmer National Identity Card” is the national ID card for Cambodian citizens, issued by the General Department of Identification of the Ministry of Interior as a single source of identification. Cambodians must possess this ID card upon reaching 15 years of age and renew their ID card every 10 years.¹⁰ In 2022, the government released 652, 843 new cards and 449, 390 replacement cards for residents aged 15 and above,¹¹ with reports indicating that “on average, the ministry can issue up to 3,000 ID cards per day.”¹²

In 2011, the government implemented a new biometric identity card¹³ which displays a person’s photo, name, sex, date of birth, date of card issuance, and duration of card validity. The holder’s complete home address, ID number, and fingerprints are stored electronically. Additionally, a scanned copy of the holder’s birth certificate and the relevant page of their family book – the physical document for the family registry – is stored electronically.

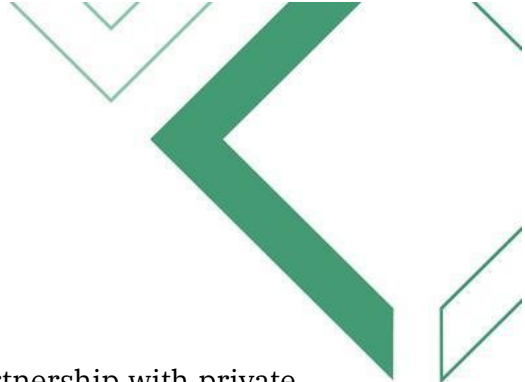
⁹ *Ibid*, n. 7.

¹⁰ Royal Government of Cambodia (2007). [Sub-decree No. 60 on Cambodian Nationality Identity Cards](#).

¹¹ Khmer Times (2022). [Ministry of Interior issued more than 650,000 ID cards in 2022](#).

¹² Khmer Times (2023). [Expired ID cards to be okayed for 2023 National Election](#).

¹³ Identity Cards.Net (2016). [Cambodia](#).



Cambodia's ID system was developed and implemented in partnership with private identity and biometric infrastructure companies, Dermalog and X Infotech.¹⁴ This included the provision of the technology related to the storage of biometric identification, citizen's ID photo, and signature, which is linked to the chips embedded into the ID cards.¹⁵

Legal Framework

Khmer ID cards are currently issued in accordance with Sub-decree No. 60 as of 2007 on "Cambodian Nationality Identity Cards."¹⁶ This sub-decree replaced the earlier Sub-decree No. 36 dated 26 July 26, 1996.¹⁷ This law limits the proof of nationality for the purpose of obtaining an ID card to (a) a birth certificate which proves that the person is a Khmer citizen; (b) a family book which confirms that his or her spouse is a Khmer national; (c) documents, judgments of a court or other evidence stating that the person was born from a father or mother with Khmer nationality, or (d) a Royal Decree proclaiming the recognition of the application for Cambodian nationality to the person.¹⁸

This sub-decree is very vague and allows the Ministry of Interior to determine most of the details of the ID card issuance process. Instructively, Article 6 of the law leaves issues related to the procedures, qualifications for application, issuance and usage of the Cambodian ID to be determined by the Ministry of Interior.

Additionally, Article 7 of Proclamation No. 2473 on Procedures and Terms of Application for Issuance and Usage of Khmer ID sets out the possible uses for the


¹⁴ Dermalog is a 'developer of biometric products and solutions,' whereas X Infotech is a 'global provider and integrator of software solutions for electronic identity (eID) documents and digital payments.' See: Dermalog. [About](#); X Infotech. [About](#).

¹⁵ Dermalog (2019). [Case Study: Biometric Solutions for Cambodia](#).

¹⁶ *Ibid.*

¹⁷ Royal Government of Cambodia (1996). [Sub-Decree No. 36 on Khmer Nationality Identity Cards](#)

¹⁸ *Ibid.*, n. 10, Article 5.



national ID card as follows: registration for ballot candidacy (voter registration), application for marriage, application for a birth certificate, application for work, application for opening a business, application for a passport, application for property ownership, and contacts with banks as well as various other sale and purchase agreements.¹⁹

National Strategic Plan of Identification (2017-2026)

Cambodia does not yet have a fully functional digital ID system but it has begun planning for one through its National Strategic Plan of Identification (NSPI).²⁰ The NSPI has a long-term vision for Cambodia – every person is to have an identity, which is now reflected in the CRVSID law. For this, the NSPI envisages the creation and operationalisation of key infrastructure: a modern, permanent, universal CRVS system that will generate reliable vital statistics; a unique identification code for every individual; and an integrated population identification system (IPIS) that will ensure that the country has a single reliable source of information about individuals and population.

The current design of the system serves primarily as a foundational ID system, and it is meant to be the sole source of identity verification.²¹ Under this system, every individual will be assigned a personal Khmer Identification Code (KIDC) at the moment of birth registration, and the code will be recorded on every identification document moving forward. The KIDC will be used to uniquely identify individuals when receiving services from the public or private sector.

Some of the most important plans related to digital identification in Cambodia, are:

¹⁹ Article 7, Proclamation No. 2473 on Procedures and Terms of Application for Issuance and Usage of Khmer ID (2007) (hereinafter referred to as “Proclamation No. 2473”; also known as “Prakas No. 2473”).

²⁰ Kingdom of Cambodia (2016). [National Strategic Plan of Identification \(2017-26\)](#).

²¹ *Ibid.*

Strategic Goal 1 - Develop an Enabling Legal Environment for Personal Identification

This goal aims to have in place a new legal environment for the new system that will be implemented, comprising two main legal frameworks: a Civil Registration, Identification and Vital Statistics Law and Sub-decree; and amendments to existing identification laws to enable the IPIS.²²

Civil Registration, Vital Statistics, and Identity Law

The CRVSID was adopted on June 21, 2023, with the law scheduled to take effect after 12 months. This law lays out the purpose, system, and principles for civil registration, identification, and vital statistics. To ensure more detailed and timely regulations, the NSPI proposes the creation of subsidiary legislation through sub-decrees. These will deal with regulating proof of life events (birth, death, etc) and ensuring the processing and access of this information to generate certificates and identification documents.

Some elements of this law include:

- Individual identification will be based on registration at birth. During registration, the individual will be assigned a personal identity code (Khmer Identification Code), which is unique to the individual and will be associated with them from birth to death. The number cannot be reused on the ID holder's death.
- The registration of an event (like birth, death, or marriage) will be made mandatory through this legal framework.

²² *Ibid*, Strategic Goal 1, pp. 28.

Integrated Population Information System Law

This law is aimed at facilitating the interaction between data sources for the IPIS system, and for cross-checking and verifying population information. This law would act as the governing law for Cambodia's digital identification system. It is proposed to include rules on replicating (from other databases) and storing data in the central registry, generating unique identification codes for all ID holders, authentication systems for use by public and private actors, and privacy and security of the system.²³

Strategic Plan 2 - Establish a Universal and Responsive Civil Registration and Vital Statistic System

The NSPI aims to establish a fully functioning web- and mobile technology-enabled civil registration system in Cambodia.²⁴

Strategic Plan 3 - Establishing the Integrated Population Identification System (IPIS)

This system is intended to act as a common integration platform for all the existing identification or e-government services and be the primary data source for population information. The system is managed by the government, and spearheaded by the Centre for Civil Registration Data Management.²⁵

Data Stored


The dataset proposed to be stored in a central registry as part of the IPIS are: name, last name, birth date, birthplace, nationality, citizenship, marital status, parents, children, declared residential address, and data about issued personal identification documents.²⁶ Notably, biometric information which is currently collected and stored

²³ *Ibid*, Strategic Goal 1, Target 3, p. 29.

²⁴ *Ibid*, Strategic Goal 3, pp. 32-37.

²⁵ *Ibid*, n. 5.

²⁶ *Ibid*, n. 20, Strategic Goal 3, p. 23.



in other identification system databases (that will be connected to the IPIS), will not be published or stored in the IPIS central registry – it will simply be used when required from those databases.²⁷ This is a privacy-enhancing measure, as it ensures that all vital information related to a citizen is not stored in the same database, which may be prone to security breaches.

The systems that are proposed to be connected to the IPIS include: (1) Khmer ID Card Management System, (2) Passport Management System, (3) Residential Management System, (4) Nationality System, and (5) Civil Registration and Vital Statistics System.²⁸

Unique ID

The Khmer Identification Code (KIDC) is proposed to be generated through the IPIS and will be assigned to each person in the IPIS. It is available for citizens, as well as non-Cambodians who live and work in the country for a prolonged period of time.²⁹ The ‘KIDC will be a 10-digit number, constructed from one reserved digit, eight random digits, plus one checksum digit that is based on the Modulus 11 algorithm.’³⁰ The reserved digit will be used to distinguish foreigners temporarily living and working in the country from citizens of the Kingdom of Cambodia.

The KIDC will be assigned at birth registration and will stay the same throughout the lifespan of a person. It will be linked to all further identification documents issued to the individual, including on their birth certificate. Further, the KIDC will also be used to integrate the Khmer ID system with the IPIS. Although limited information is available about what the government intends to do with this, some of its stated goals include the development of ‘voter lists, other related needs, (such as law enforcement), or private sector needs while IPIS will become fully functional.’

²⁷ *Ibid.*

²⁸ *ibid.*, n.5.

²⁹ *ibid.*, n.20, Strategic Goal p. 39.

³⁰ ISSN International Network. [Calculating the check digit.](#)

Population Registry

The NSPI envisions the creation of a national central database, the Population Registry, which will store the main data about the population of Cambodia.³¹ It will be the central data hub of the IPIS and will have developed functionality for ensuring information exchange between the CRVS, Khmer ID System, Passport System, Nationality System and Residential Management System. The Population Registry will replicate data to the Information Distribution System for authorised and secure disclosure to the public and private sectors.

Residential Management System

The NSPI aims to implement a Residential Management System, which will be the single source of information on individual addresses and familial compositions for the Integrated Population Identification System. The Residential Management System will be integrated with the IPIS to update the data on the place of residence in the Population Registry.


Nationality Management System

A nationality management system will be implemented that will help trace the acquisition of Khmer Nationality and the issuance and storing of nationality documents.

Identity Verification and Authentication Platform

After the IPIS has become operational and accumulated enough reliable records on the population, the NSPI envisages the launch of a data distribution service and an authentication platform. At this point, the IPIS and related systems will form a fully functional digital identification platform. It is difficult to ascertain the possible harms

³¹ *Ibid*, n.20, p. 39



of the system since it is at a nascent stage, but some of the proposed features of this platform include:


- Distribution of data is to “authorised users” and based on contracts with the information recipients specifying the rights and responsibilities of the GDI, the operation of the data distribution system and information recipients.³²
- Facilitate citizen participation in the implementation of this plan by including civil-society organisations and non-governmental organisations (NGOs) in the CRVS governance structure.
- Launch e-government and public services on the platform
- All the civil registration and residential registration services will be made accessible online, with the possibility for electronic authentication and digital signatures.
- Enable digital payment and electronic transfers to pay for civil registration and for services related to population information verification

Monitoring and Governance

The implementation of the plan is the responsibility of the National Steering Committee on CRVS and Identification (NSCI). The NSCI comprises members from several different government ministries, along with one NGO representative involved in the civil registration area and one development partner representative to participate as observers or advisers or other necessary activities.³³ It remains to be seen how effective their participation will be, but it is a move in the right direction to involve a broad set of stakeholders capable of holding the government to account in

³² *Ibid*, n.20, p. 43.

³³ *Ibid*, n.20, p. 49.



the implementation committee. If nothing else, it could increase the transparency and accountability of the committee.

Implications of Cambodia's ID system and National Strategic Plan of Identification 2017–2026

Discrimination and Exclusion


Assigning rights and access to services on an entirely new system always runs the risk of excluding marginalised people or further entrenching discrimination. When countries are considering new, computerised/digitised forms of registration and legal documentation, special measures must be taken from the time of designing the system to ensure that fair and impartial access is guaranteed to those who will face difficulties in otherwise accessing it.

In Cambodia, registration for the Khmer ID (and the proposed system under the NSPI) currently relies heavily on birth certificates and birth registration (which is when the KIDC will be issued.) However, there have been many reports of inadequate access to birth registration by some minority communities, such as Vietnamese residents that have been living in Cambodia.³⁴

In a study conducted among these residents, most of them had lost vital documents that they obtained under the previous regimes when the Khmer Rouge forced them to abandon their homes and possessions.³⁵ Other long-term residents claimed they had no access to birth registration, not only because of a low level of awareness among their community but also because local officials did not register the newborns of the

³⁴ Christoph Sperfeldt (2020). *Minorities and Statelessness: Social Exclusion and Citizenship in Cambodia*.

³⁵ *Ibid.*



Vietnamese (under the presumption that it was only Cambodian nationals that could register their children.)³⁶

The government should allow other proof of identity documents for individuals to be able to obtain a Khmer ID. For instance, under the now defunct GOV.UK Verify (Verify),³⁷ replaced by GOV.UK One Login, applicants in the United Kingdom were allowed to show records from mobile phone providers, credit agencies, or the Driver and Vehicle Licensing Agency.³⁸ This was intended to target those who do not have government documents.

Similarly, in India, under the Aadhaar system, applicants who do not have birth certificates or other government ID documents were allowed to register through the ‘Introducer system.’ This involves permitting an Introducer, typically a member of a community or village who is well known, to stand as a verifier of the applicant’s identity.³⁹ This is intended to target individuals in remote areas or marginalised communities that otherwise would not be able to access the Aadhaar system as they do not have proof of identity or address.

Identity documentation in Cambodia has also followed some dangerous practices, where registration for a legal document is accompanied by systematic confiscation of prior documentation that authorities deem to be “irregular administrative documents.”⁴⁰ The Ministry of Interior identified more than 70, 000 mostly Vietnamese ‘foreigners’ holding such irregular documents.⁴¹ There have been other such reports of authorities confiscating legal documents previously held by

³⁶ Minority Rights Organisation (2016). [Report on Access to Birth Registration for Marginalised or Vulnerable Populations: A Case Study on Ethnic Vietnamese Minority Communities in Cambodia.](#)

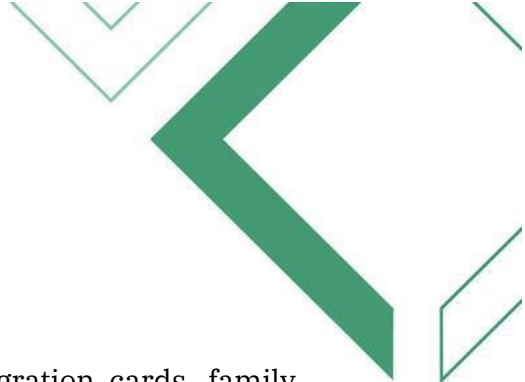
³⁷ United Kingdom. [GOV.UK Verify - GOV.UK \(www.gov.uk\)](#); United Kingdom. [GOV.UK One Login.](#)

³⁸ The Center for Internet and Society, India (2019). [Mapping Digital Identity Systems: UK.](#)

³⁹ The Center for Internet and Society, India (2020). [Mapping Digital Identity Systems: India.](#)

⁴⁰ Based on Sub-Decree No. 129 on the cancellation and withdrawal of irregular Cambodian administrative documents possessed and used by foreigners.

⁴¹ The Phnom Penh Post (2017). [Interior Ministry Identifies 70,000 “Improper” Citizens, Mostly Ethnic Vietnamese.](#)



Vietnamese residents, including birth certificates, old immigration cards, family books, and other identification documents. Additionally, there have also been cases of Cambodian authorities taking away Cambodian ID cards from people they deem to be ethnic Vietnamese, with little other investigation as to their legal status.⁴²


These examples demonstrate one of the major problems with having one centralised ID system that acts as the platform for all other documentation and services. If an individual's access to the system is denied – either by never getting an ID or by having it taken away by the government for “irregularities” – it becomes impossible to live a regular life in the country. If special measures are not taken to include marginalised and excluded people from the Cambodian ID system, their statelessness and discrimination will increase disastrously.

Conclusion and Recommendations

Since most of Cambodia's digital ID system is still in the planning stage, with limited publicly available information, it is difficult to ascertain harmful practices or recommend policy changes. However, what is clear from Cambodia's history with identification systems is the risk of discrimination and exclusion that a new digital ID system can bring, especially for migrants from bordering states.

Typically, digital ID systems in other countries (such as India, Estonia, the United Kingdom, amongst others) are not closely linked to nationality or citizenship, allowing residents (and even e-residents in the case of Estonia) to access the system. This distinction between citizenship records and the digital ID platform is important to ensure maximum participation in the digital ID system and limit discrimination

⁴² *Ibid*, n. 34.



against some communities. It will also remove any fear or apprehension on the part of the ID applicants regarding their citizenship status.

Recommendations

We urge the Government of Cambodia:


- To separate nationality and citizenship records from its digital ID and authentication platform, and allow more than one way for persons residing and working in Cambodia to get a Khmer ID or otherwise be part of the IPIS platforms.
- To expand its entry points, allowing other ways to register for an ID. Currently, birth registration is the default way to get a KIDC, which in turn is required to be part of the IPIS.
- To provide special measures for people who do not have government identification/records (such as birth certificates) to prove their identity through other means and access IPIS. Specifically, the governing policy should allow other proof of identity documents for individuals to be able to obtain a Khmer ID.

DIGITAL ID IN INDONESIA

Summary

The identity (ID) system in *Republik Indonesia* (Republic of Indonesia or Indonesia) currently functions as a digitized version of the country's foundational ID systems, the population registration and civil registration systems. The *Kartu Tanda Penduduk Elektronik* (the electronic-KTP system or electronic national ID card) operates as a digital application built upon the foundational population database. Although efforts are currently underway, the transition from the e-KTP to the Digital KTP, the country's planned national digital ID, has not yet been deployed across the country. The Digital KTP will involve the transfer of the e-KTP to mobile phones.

The current national ID system gives rise to concerns about the potential for extensive surveillance and security risks stemming from the vast data collection and the close link between civil registration and the digitized national identity. To address these challenges, stringent measures must be implemented in the governing laws to limit data types and duration, control access by public and private actors, and define disclosure circumstances. Robust cybersecurity and disaster mitigation policies are also essential.



Additionally, relying solely on one specific identification document, such as the e-KTP, poses a risk of excluding and marginalizing certain segments of the population, considering the importance of this document for accessing essential services. The e-KTP national law and policy should be amended to accept multiple, and alternative forms of identity proof during registration. These changes could introduce inclusivity into the identity system, and eliminate barriers faced by marginalized communities during the registration process.


Historical Context

Indonesia's current civil registration system dates back to its colonial history, evolving into two distinct versions that were shaped during the periods of Dutch and Japanese colonization.¹ The Indonesian National Card, or the *Kartu Tanda Penduduk*, was mandated as a proof of identity for citizens and residents aged 17 and older (or upon marriage, for persons aged below 17).² It builds on a long tradition of civil registration – the recording of births, deaths, and marriages – that was introduced in 1945.

In 2011, the electronic KTP (e-KTP) was launched nationwide, managed by the Ministry of Home Affairs and the *Ditjen Dukcapil* (the General Directorate for Population and Civil Registration). The e-KTP contains a microchip, biometrics (fingerprint, iris and facial recognition), and a unique serial number, and can be used for multiple applications for government services. The biometrics system was introduced to remove duplicates in the database, and enable identity verification for Indonesians.

¹ Shahril Budiman. [The Analysis of Indonesia Policy on National Identity Card: Lesson Learnt from Selected ASEAN Countries.](#)

² Law of the Republic of Indonesia (2006). [Undang-undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan](#) ["Law Number 23 of 2006 on Population Administration" (in Indonesian)].



The e-KTP is now the basis for the issuance of Indonesian passports, driving licenses, SIM cards, taxpayer identification numbers (*Nomor Pendaftaran Wajib Pajak* or NPWP), insurance policies, land ownership certificates, and several other identity documents.³ According to the 2017 World Bank ID4D-Findex survey, 96% of Indonesians aged 16 and over have a KTP or an e-KTP.⁴

World Bank Loan (Identification for Development, ID4D)

Towards the end of 2022, the Indonesian government began negotiations with the World Bank for a USD 250 million loan to ‘strengthen the country’s civil registration system and increase the use of biometric digital identification for accessing public and private sector services.’⁵ This effort will be implemented under a project known as the ‘ID for Inclusive Service Delivery and Digital Transformation in Indonesia.’ This project is intended to convert Indonesia’s existing foundational, digitised, ID system into a complete digital ID system, granting both government and private services access to the system. The details of this system and the proposed digital ID framework are yet to be seen.

Although the Indonesian foundational ID system is digitized and includes the collection and use of biometric information, the country lacks a digital ID system and framework for digital or online authentication. Currently, Indonesian ID holders are asked to verify themselves either through demographic verification mechanisms or by taking a selfie of themselves holding their e-KTP.⁶ Consequently, a large part of the World Bank’s project focuses on using the existing population registration and civil

³ *Ibid*, Article 13, Law no. 23/2006.

⁴ The World Bank (2019). [Global ID Coverage, Barriers, and Use by the Numbers: An In-Depth Look at the 2017 ID4D-Findex Survey](#).

⁵ Biometric Update.Com. [World Bank proposes \\$250M for Indonesia digital ID for public and private service access](#).

⁶ The World Bank. [Project Information Document \(PID\), Appraisal Stage](#).

registration (PR/CR) systems to act as a platform for national digital ID and identity verification services.

Table 1: Summary of World Bank (ID4D) Project

ID for Inclusive Service Delivery and Digital Transformation in Indonesia

This project has the following components:

- Component 1 – Population and civil registration
- Component 2 – Identity verification, digital identification, and ICT infrastructure
- Component 3 – Utilization and adoption
- Component 4 – Institutional and human capacity
- Component 5 – Project Management and coordination.⁷

Identification Systems and Policies

The collection and management of personal data through the e-KTP system in Indonesia is governed by Law No. 23 as of 2006 on Administration of Population and Civil Registration (Law No. 23 as of 2006 or the Population Administration Act),⁸ later updated by Law No. 24 as of 2013 (Amendment Law).⁹ The main components of Indonesia’s foundational ID system as established by this law include the:

- Population Administration Information System (“SIAK”) database
- Unique national ID number (“NIK”) issued at birth registration
- Electronic national ID card (“e-KTP”) available from age 17: residents are mandated to obtain the e-KTP when they reach the age of 17 or if they get

⁷ *Ibid.*

⁸ *Ibid.*, n. 2

⁹ Law of the Republic of Indonesia (2013). [Amendment to Law Number 23 Year 2006 on Population Administration.](#)

married. A resident is defined as an Indonesian Citizen and Foreigners residing in Indonesia.¹⁰

- Family card (KK), and
- Various certificates for births, deaths, marriages, and other vital events.

The data collected through the comprehensive foundational PR/CR systems – including e-KTP – is vast.¹¹ The e-KTP contains personal and sensitive personal data, including the NIK, full name, facial photo, gender, residential address, place and date of birth, religion, occupation, blood group, citizenship, marital status, signature of the holder, expiration date of the e-KTP, and biometric fingerprints.¹²

Under Article 13 of Law No. 23 as of 2006, it is mandatory for all residents to have a NIK, and this must be included in every population administration document. The NIK facilitates the issuance of passports, driver's licenses, insurance policies, and all other identity documents,¹³ including tax numbers.¹⁴ Registration and data updates, including changes in address, are effected by *Dinas Kependudukan dan Pencatatan Sipil* (*Dinas Dukcapil* or the Population and Civil Registration Agency) which reports to local governments.¹⁵ Both *Dinas Dukcapil* and *Ditjen Dukcapil* make population data available to institutional users. At the aggregate level, this allows the production of statistics, and at the individual level, this allows a service provider, such as a government agency or bank, to verify the identity of a client.

¹⁰ *Ibid*, n. 2, Article 63; *Ibid*, Article 1.

¹¹ This includes personal data, contact data, biometric data, medical data, document data, family data, employment data, educational data, and religion/belief data, amongst others.

¹² Center for Digital Society (2019). [e-KTP and Personal Data Protection: Are We Ready?](#); *Ibid*, n. 9, Article 64.

¹³ *Ibid*, n. 2, Article 13 (3).

¹⁴ Mahkamah Konstitusi Republik Indonesia (2023). [MK Gelar Sosialisasi Validasi NIK Sebagai NPWP](#). (*Indonesian*)

¹⁵ *Ibid*, n. 2, Articles 14-22.

Implications of Indonesia's ID system

Exclusion and Discrimination

The KTP, and its electronic version, is considered indispensable to life in Indonesia. Residents need the ID to access basic public services like health care and education; participate in elections; register births, deaths, marriages; apply for SIM cards, jobs and bank accounts. The Population Administration Act even mandates that the government provide all public services based on the NIK number.¹⁶ This has resulted in the exclusion and discrimination of groups and communities, on the basis of religion and gender identity. Consequently, this has created a community of vulnerable people that live on the margins of society in Indonesia, unable to access most public or private services.

Religion

The inclusion of religious information on the e-KTP card has been a source of problems for Indonesians. The Amendment Law specifies that residents whose religion is not officially recognised under Indonesian laws have to be treated similarly to the rest of the population, and registered in the system.¹⁷ This is further entrenched by the Indonesian Constitutional Court Decision (97/PUU-XIV/2016) that allows the inclusion of indigenous beliefs (*aliran kepercayaan*) in the national ID.¹⁸ Despite this, religious communities that are not officially recognised in Indonesia have claimed to be subject to incidents of discrimination.

In 2017, representatives from the Ahmadiyah community filed a formal complaint against a local government in the West Java district, alleging that they were not being

¹⁶ *Ibid*, n. 2, Article 64(4).

¹⁷ *Ibid*, n. 8, Article 14.

¹⁸ The Constitutional Court of the Republic of Indonesia (2016). [Verdict Number 97/PUU-XIV/2016](#).

issued ID cards unless they renounced their faith.¹⁹ This was not solely due to the fact that the Ahmadiyyah faith is not among the six religions officially recognized in Indonesia.²⁰ Instead, a “conservative turn” and “godly nationalism” – as scholars dub it – have recently caused Ahmadiyyah to not be considered as Islam by the more mainstream school of Sunni Islam in Indonesia.²¹ In this complaint, the religious community claimed that their lives were impacted by the lack of a national ID, as they were unable to access most government services, including hospital treatment and registration of marriage, among others.²²

Gender Identity

In 2019, a transwoman who had been expelled from her family and therefore did not have an e-KTP was unable to access health services and died of complications from HIV/AIDS.²³ The digitisation of this system has only furthered their invisibility, as trans people are either absent or misidentified from all databases. With government policy now being determined based on these databases, the marginalization of people with different gender identities is all but guaranteed.

Health

During the COVID-19 pandemic, vaccinations were given on the basis of the e-KTP, therefore excluding a large chunk of the marginalized population from essential health services.²⁴

¹⁹ Human Rights Watch (2017). [Indonesia's Ahmadiyah Push Back Against Discriminatory Laws: Conversion Requirement for National ID Cards Prompts Protest](#); Reuters (2017). [Indonesian Islamic sect say they're 'denied state IDs' over their beliefs](#).

²⁰ Law of the Republic of Indonesia (1965). [Nomor 1 Tahun 1965 Tentang Pencegahan Penyalahgunaan Dan/Atau Penodaan Agama \(Blasphemy Law\)](#).

²¹ EngageMedia. [New report on religious freedom in Indonesia: Civil society must grow more critical of intolerance online](#).

²² Reuters (2017). [Indonesian Islamic sect say they're 'denied state IDs' over their beliefs](#).

²³ Adi Renaldi. [Indonesia's invisible people face discrimination, and sometimes death, by database](#).

²⁴ *Ibid.*

Privacy and Data Protection

On October 17, 2022, the Indonesian government passed Law No. 27 as of 2022 concerning Personal Data Protection (the “PDPA.”) This was the first attempt of a comprehensive data protection law in Indonesia. The applicability of the PDPA of 2022 to the e-KTP is not properly established. However, the law requires data controllers, including the administrators of Indonesia’s foundational ID systems, to conduct a data protection impact assessment for high-risk processing of personal data.²⁵

Prior to the enactment of the PDPA, 2022, sector-specific regulations provided for the collection and use of personal data in the e-KTP system, wherever relevant, and included the:

- Electronic Information and Transactions Act (“EIT Law”)²⁶
- Government Regulation regarding the Operation of Electronic Systems and Transactions and its implementing regulations
- Minister of Communication & Informatics Regulation regarding the Protection of Personal Data in an Electronic System.²⁷

Notably, the governing law of the e-KTP system, the Population Administration Act, expressly provides for the protection of private data of residents. Articles 85 and 86 task the implementing authorities with storing and protecting this private data. Prior to the Amendment Law, Article 84 of the Population Administration Act defined *private data* as encompassing ‘the KK number, NIK, birth details, information about one’s physical or mental disability,’ amongst others.

²⁵ HHP Law Firm (2022). [Indonesia: The Personal Data Protection Law is Finally Here. What Does That Mean to Your Business?](#)

²⁶ Law of the Republic of Indonesia (2008). [Law No. 11 of 2008 regarding Electronic Information and Transactions Act](#)

²⁷ Republik Indonesia (2016). [Peraturan Menteri Komunikasi dan Informasi no. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik](#), Pasal 3.

Following the implementation of the Amendment Law, Section 21 (amending Section 84 of the Population Administration Act), the definition of *personal data* was altered to mean biometric data (iris scan, fingerprints), physical/mental disability, signature and other data elements “constituting the flaws of a person.”²⁸ In effect, this amendment means that personal data, such as the NIK and e-KTP number, are not protected as personal/private data under this Act.

It is also unclear how many bodies have access to data in the e-KTP system.²⁹ In 2021, the Ministry of Home Affairs disclosed that 3,904 public bodies, which comprise 2,178 central ministerial/agencies and 1,726 local government institutions, were given access to the database.³⁰ During this time, there were several instances of data breaches and the misuse of information in the e-KTP system.³¹

- In 2017, former minister Tjahjo Kumolo reportedly shared the e-KTP data of a human rights defender, Veronica Koman, who publicly criticized the Indonesian government.³²
- In May 2020, reports detailed the leak of information related to millions of Indonesian residents from the 2014 Election Permanent Voters List. This data included sensitive information such as resident name, family card number, NIK, place and date of birth, home address, and other personal data.³³
- Such data leaks also affected government bodies:
 - In 2021, four local government agencies that had access to the database reportedly suffered from data breach incidents.³⁴

²⁸ *Ibid*, n.2, Article 84.

²⁹ *Ibid*, n.2, Article 79: this allows the Minister to grant right of access to officers and users in the system.

³⁰ Ministry of Home Affairs (2021). [From 30 to 3,904 Institutions, Integration of National Data Has Progressed.](#)

³¹ TFR (2021). [The twists and turns of personal data security in Indonesia.](#)

³² BBC (2017). [Tindakan Mendagri menyebarkan KTP menuai kecaman.](#)

³³ The Jakarta Post (2020). [Calls mount for comprehensive audit into data breach affecting 2.3 million voters.](#)

³⁴ Tempo.co (2021). [Dukcapil data in 4 regions allegedly leaked, DPR members ask the police to act.](#)

- In 2022 alone, at least 40 incidents of data leaks affected 60 public agencies in Indonesia.³⁵


Conclusion and Recommendations

Currently, Indonesia's foundation ID system encompasses both the population registration and civil registration (PR/CR) systems. The country's national ID card, the e-KTP, is simply a digital application built atop the foundational PR/CR database. This is subject to change, given the World Bank's influence and funding under the '*ID for Inclusive Service Delivery and Digital Transformation in Indonesia*' project. Illustratively, reports emerged in 2023 that the government has commenced its transition towards a fully-fledged digital identification platform, through the deployment of the Digital KTP.

This case study argues that the integration of a civil registration system with a digital ID platform carries substantial risks for residents in Indonesia. The extensive data collected by the civil registration system for each resident, combined with the additional data generated by a digital identity authentication/verification platform, bestows significant surveillance capabilities upon the entity in possession of such information. Simultaneously, such a system also has security risks as this data can be breached or hacked.

The KTP, and its electronic version, is indispensable to life in Indonesia, because essential services can only be accessed if one possesses the national ID card. This can result in consequential exclusions, where people who are unable to access the ID continue to live on the margins of society, thus exemplifying their exclusion. Unless

³⁵ SAFEnet (2023). [\[Report\] The Digital Rights Situation in Indonesia Had Worsened.](#)



the government moves away from mandating possession of the current e-KTP, the ongoing incidents of exclusion and discrimination will worsen.


Recommendations

We urge the government of Indonesia to:

- Issue a directive clarifying that the Personal Data Protection Act (2022) applies to all personal and sensitive data collected and processed under the national ID law, the Population Administration Act.
- Amend the e-KTP law, and any other applicable laws and policies, to accept multiple, and alternative forms of identity proof during registration.
- During the deployment of the Digital-KTP, pay special attention to the current causes of exclusion (e.g., religious beliefs or identities), and deploy identity verification that is inclusive *for all*.

We urge the Ditjen Dukcapil, the implementing agency under the Ministry of Home Affairs, to:

- Establish comprehensive cybersecurity and disaster mitigation policies to mitigate data breaches to the system or failure of the system.
- Put in place measures to limit the
 - types and duration of data stored,
 - access that public and private actors have, and
 - circumstances in which disclosures of information from the system may be made.



DIGITAL ID IN THE REPUBLIC OF MALDIVES

Summary

The current digital applications of the national identity (ID) in *Divehi Raajjeyge Jumhooriyyaa* (the Republic of Maldives or Maldivian Islands or Maldives) are not properly regulated within the existing national ID law, raising concerns about the potential misuse of data collected. A comprehensive framework is crucial before implementing a biometric digital ID system. To achieve this, the country should introduce a set of laws and policies governing the ID program, data privacy, and cybersecurity.

Further, careful consideration is required for recent updates proposing a government-issued unique digital ID credential combining multiple functional identities, as overreliance on one form of identity may lead to significant exclusion, especially in a country still developing its internet infrastructure and building its technological literacy. The involvement of the World Bank in enhancing trust in online transactions may aid progress towards a more robust and regulated digital ID system.

Historical Context

Over the past decade, the telecommunications (telecoms) infrastructure and the use of digital technology has rapidly grown in Maldives, with over 60% of the population now using the internet.¹ The COVID-19 pandemic accelerated the digital shift in a country with an estimated population of 457,900 in 2023.² As part of the government's attempts to boost economic growth and address emerging challenges, Maldives created a National Resilience and Recovery Plan (NRR) 2020–2022.³ The NRR prioritizes the establishment and adoption of a National Digital Identification System, which would “enable the adoption of biometric technologies in identity management systems and introduce contactless identification cards.”⁴

Maldives has a Civil Registration and Vital Statistics (CRVS) system, which is tasked with ensuring the registration of births and deaths in the country. The Department of National Registration (DNR), an office under the Ministry of National Planning, Housing, and Infrastructure,⁵ is responsible for collecting birth and death forms and entering these in an online database.⁶ The DNR is also responsible for issuing the national identity (ID) card, the primary identification document in the country. As of 2017, the birth registration rate was at 99%, and the DNR estimates that ID coverage among adults is also close to universal.⁷

¹ World Bank (2022). [Realising a Digital Future for Maldives](#).

² Britannica (2023). [Facts & Stats](#).

³ High Commission of Maldives. [President Holds Press Conference, Briefs Media on National Resilience and Recovery Plan](#).

⁴ The President's Office (2022). [The President decides to establish a National Digital Identification System](#).

⁵ Ministry of National Planning, Housing, and Infrastructure.

⁶ The Economic and Social Commission for Asia and the Pacific (ESCAP) (2022). [Assessment, Analysis and Redesign of Civil Registration and Vital Statistics Processes - Maldives Report on the implementation of Stage 1: Assessment, analysis, and redesign of the CRVS Systems Improvement Framework](#).

⁷ The World Bank (2022). [Project Appraisal Document - MV: Digital Maldives for Adaptation, Decentralization and Diversification \(P177040\)](#), p. 5.

Identification Systems and Policies

The national ID card issued by the DNR does not have features that would enable digital verification⁸ or authentication. In 2012, the National Centre for Information Technology (NCIT) introduced the “eFaas,” the Maldives’ national digital identity platform, which allows users to verify their identity digitally, in-person and online.⁹

As of December 2022, the NCIT was testing digital ID multi-application cards ‘One-Gov’ for 500 Android users,¹⁰ which can be used for the eFaas authentication service for government digital services.¹¹ In March 2023, President Ibrahim Mohamed Solih announced that they would begin rolling out digital ID cards and launch ‘One-Gov’, an online government service where ID holders can access the government and public sector online services. This digital ID card is integrated into the eFaas application (app) via biometric matching, primarily using the user's face and electronically comparing it to an existing facial image and its attached personal information within the app’s database.¹² Due to this biometric linkage, the app enables all cards issued by a government agency to digitally access an individual's personal information.¹³

Current Digital ID Project and World Bank Funding

In June 2022, the World Bank’s Board of Executive Directors approved a USD 10 million grant to the government of Maldives for the “Digital Maldives for Adaptation, Decentralization and Diversification” Project. This project is aimed at improving digital technologies in Maldives, and will support the government in strengthening the legal, regulatory, and institutional frameworks for broadband internet

⁸ “The process of establishing confidence in user identities presented digitally to a system.” NIST, Computer Security Resource Center. [Digital Authentication](#).


⁹ National Centre for Information Technology. [eFaas](#).

¹⁰ Atoll Times (2023). [Digital ID trial opens with 500 Android app slots](#).

¹¹ PSM News (2022). [Maldives to begin use of digital identification cards](#).

¹² National Centre for Information Technology. [E-Faas Privacy Policy](#).

¹³ PSM News (2023). [Digital ID cards to be used from March onwards](#).



connectivity and infrastructure, data governance, and the digital economy.¹⁴ The project will be implemented by the Ministry of Environment, Climate Change and Technology, in partnership with the Communication Authority of Maldives, NCIT, and DNR.

Among other things, this project has the express goal of enhancing trust and efficiency in online transactions and service delivery through the modernisation of existing identity management software and hardware. The project also proposes to introduce a digital ID system with a new digitally-enabled ID credential to enable secure data sharing and authentication online.¹⁵ Under this project, the financing document also seeks to strengthen the legal and regulatory frameworks governing data protection, cybersecurity and cybercrime, electronic transactions, identification and civil registration in the Maldives.¹⁶ To that end, the government of Maldives recently passed the Electronic Transactions Act, 2022,¹⁷ and the Birth, Death and National ID Registration Act, 2022.¹⁸

In February 2022, President Ibrahim Mohamed Solih announced that the government will be establishing a National Digital Identification System (NDIS) in accordance with the administration's National Resilience and Recovery Plan (NRR) 2020–2022.¹⁹ This identification system will be developed and maintained by the NCIT and the DNR. It will enable the adoption of biometric technologies in DNR's identity management systems, and introduce contactless identification cards. NICT and DNR are also

¹⁴ The World Bank (2022). [World Bank Supports Maldives to Leverage Digital Technologies for Development and Climate Resilience](#).


¹⁵ World Bank (2022). [MV: Digital Maldives for Adaptation, Decentralization and Diversification \(P177040\) - Project Information Document](#), sub-component 2.1.

¹⁶ *Ibid*, sub-component 1.1.

¹⁷ The Republic of Maldives (2022). [Electronic Transactions Act, 2022](#).

¹⁸ Maldives Moot Court Society (2022). [Maldives enacts a new Act pertaining to Birth and Death registration and the issuance of Birth Certificates and Maldivian National Identity Cards \[Law no. 23/2022\]](#).

¹⁹ The President's Office. [Press Release: The President decides to establish a National Digital Identification System](#).



expected to develop digital identification applications for smartphones and extend the use of the digital identification platform to the private sector.

As part of preparations to launch the proposed digital identification cards, the DNR announced the redesign of the national ID card as a ‘smart card’ with modern security features in June 2022.²⁰

Implications of National Digital Identity Platform (eFaas)

Since the eFaas system was launched in 2012, around 137,000 people have registered, according to the NCIT.²¹ Currently, eFaas acts as the Maldivian digital ID with roughly 159,900 active users and 85 digital service portals ranging from health platforms to job centers,²² allowing users online authentication of their identity. In the absence of a comprehensive digital ID law governing this, this report analyzes the terms of service and privacy policy that the NCIT has published on the eFaas website.

Terms of Service and Privacy Policy²³

The Terms of Service act as the agreement between the administrator of the eFaas system, the NCIT, and the ID holder. The Privacy Policy published on the eFaas website sets out eFaas’s policies and procedures on the collection, use and disclosure of ID holders’ information.

Data Collected


eFaas collects data about ID holders from three different sources:

²⁰ PSM News (2022). [National identification card to be redesigned.](#)

²¹ Maldives News Network (2023). [Over 130,000 people enrolled for eFaas in four years: NCIT.](#)

²² *Ibid*, n. 9.

²³ National Centre for Information Technology (2023). [Privacy Policy](#); National Centre for Information Technology. [Terms and Conditions.](#)

- 
1. Directly from users: Data collected when the user registers for their eFaas account, or is required to provide additional identity proof to strengthen their profile.²⁴
 2. Indirectly from users: Data recorded about user's device and system interactions when they use their eFaas account.
 3. Third-party sources: Data collected from government authorities to verify and validate the user's identity information. The eFaas identity system is connected to several government registries.

Nature of Personal Information Collected

A wide variety of personal information is collected, including: (1) date of birth, (2) address, (3) contact details, including email address and phone number, (4) data contained in the Department of National Registration, Ministry of Economic Development, and Maldives Immigration, and other existing identity documents of the user. The data collected by eFaas here includes (*non-exhaustively*): (a) the type of document, (b) document issuer, (c) document numbers, (d) effective dates, (e) photographic images, and (f) signatures.


Further, biometric images of the user's face are also collected, with this type of data generally being classified as sensitive personal information under international human rights and data protection laws.²⁵

While validating users' documents, eFaas also keeps a record of the document, the information verified, and the authentication response.

Biometric Data

²⁴ *Ibid.*

²⁵ European Commission. [What personal data is considered sensitive?](#)



Biometric data refers to ‘data relating to the physical, physiological or behavioral characteristics of an individual which allow their unique identification, such as facial images and fingerprints. Due to its identifiable nature and high probability of abuse, this data should ideally be processed and stored in very exceptional circumstances.’²⁶

The eFaas system collects users’ biometric data (face images) to perform biometric matching, where it electronically compares users’ personal information and facial image against users’ ‘photographs on submitted ID documents’ to verify their identity.²⁷ Pictures and videos taken during facial recognition are stored with the face verification service vendor, who provides facial recognition service for eFaas for the purpose of verification and authentication, and which is securely deleted after five years.


The collection and use of biometric information poses significant privacy and security risks for individuals. Critically, this data collection should not be conducted without a comprehensive legal framework that satisfies the legality, necessity, and proportionality threshold under international human rights law. Regulations should at the very least demonstrate a clear lawful basis for the processing of biometric data for legitimate purposes, and limit the collection of data for strictly necessary, and clearly defined, circumstances. Additionally, existing ID systems should be buttressed by implementing sound technology and cybersecurity systems.

Indirect Data Recorded

There are concerns that digital ID systems have the potential to aid surveillance efforts targeting vulnerable groups, due to its ability to distinguish and single out individuals using their biometric data and associate their activities with said data. Contextually, Maldivian human rights groups have increasingly become targets of

²⁶ The World Bank Group’s Identification for Development (ID4D) Initiative (2022). [Primer on Biometrics for ID Systems](#).

²⁷ National Centre for Information Technology (2023). [About eFaas](#).



surveillance, harassment, threats of violence, and blasphemy allegations, including from extremist non-state actors.²⁸


The eFaas system records data based on the user's activity within the system. According to the Privacy Policy, the data recorded includes:

1. Information about the user's device and browser, such as operating system and user session.
2. IP address and internet provider information.
3. The date and time of use of the authentication service.
4. Successful and unsuccessful attempts at authenticating.

These logs of a user's activity are typically kept within the e-Faas system to ascertain what service providers are using the authentication service, and in what instances user data was shared with them. However, such authentication records would essentially allow anyone who can access it to create a trail of where the ID holder has used their ID, and for what purposes.

This issue has been considered in other countries that have deployed digital ID systems. It was argued before the Indian supreme court that transaction data in authentication records would enable the state to track the location of an ID holder seeking authentication and ascertain the activity they are engaging in. It was argued that the concentration of important information such as the user's ID number, their name, the authentication response (whether authentication was successful), and the requesting entity's IP address enables the collecting party, in most cases the government, to profile the user. The court in this case agreed that the collection and

²⁸ Freedom House (2022). [Freedom in the World Report 2022: Maldives](#).



maintenance of data such as the IP address of the transacting parties is a violation of the ID holder's privacy.²⁹

While the collection and storage of authentication records is arguably a security feature that restricts access to the ID system only to authenticated users or third parties, the collection of such data must also be proportionately balanced against privacy protections.³⁰ Critically, the collection of indirect data, if combined with other data captured in the eFaas system, can support users' monitoring and surveillance activities, posing a significant risk to users' privacy rights.

Storage of Data

A digital ID policy must detail how data is stored, and for how long. The principle of data minimisation, which should be strictly adhered to especially by systems that collect and process vast amounts of data such as digital ID systems, urges data controllers or processors to minimize the collection and storage of data to what is strictly necessary. Integral to this, is the requirement for the deletion of any data that is no longer required.

Notably, the biometric face recognition data that is stored with the third-party vendor, Sum and Substance Ltd, is securely deleted after five years.³¹ There is little information regarding the government's contract with the vendor pertaining to the protection of the identifiable and sensitive data stored. This raises concerns regarding the privacy and security of users, especially when personal data protection relies solely on a contractual agreement. This approach can be particularly risky as it leaves citizens in a highly vulnerable position with minimal accountability for potential misuse.

²⁹ *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 232, ¶ 144; Centre for Internet and Society (2020). [Judicial Trends: How Courts Look at Digital ID Programs](#).

³⁰ HID Global. [Authentication Records](#).

³¹ *Ibid*, n. 27; Sum and Substance Ltd (2023). [Privacy Notice \(Sumsub Service\)](#).

Disclosures

With the vast data that a digital ID system collects, the access it allows to state and non-state third parties, especially for law-and-order purposes, forms a crucial part of its policy. The requirement of a judicial order for disclosing information under the eFaas system to a third party should be a minimum requirement instituted into its governing framework.


The eFaas privacy policy describes a few situations in which it may disclose information without the user's consent:

1. Data about the ID holder's use of the eFaas system may be accessed and shared to detect, manage and investigate fraudulent activity which may lead to criminal prosecution, and
2. Any type of personal data collected/accessed by the system may be shared with third parties "if authorized or required to by law."

These broad disclosures pose a risk to the privacy rights of ID holders, especially where this data is accessed and used for law-and-order purposes. Typically, persons of interest (or suspects) in criminal investigations have the right to post-surveillance notification that facilitates individuals to exercise their right to legal redress where their right to privacy has been violated.³² Notably, allowing access to a civilian information system that is otherwise connected to the day-to-day life of a citizen can pose a grave violation of their privacy, and where post-surveillance notification is not provided, this can thwart the right to legal redress and the right to privacy.

Further, in other countries where data-intensive digital ID systems have been implemented, courts have insisted on the inclusion of safeguards or controls in disclosure provisions. In Jamaica, a case on the constitutionality of the national digital

³² [AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services](#) [2021] ZACC 3.



ID system was heard by the Supreme Court. The Supreme Court held that vague terms used in the disclosure provision - “when authorized by law”, or “for the detection and prevention of crime” – was an unconstitutional violation of ID holders’ privacy rights.³³ Similarly, in Mauritius, disclosures from the digital ID system were allowed for reasons of national security and the prevention of crime, in the absence of any judicial oversight. Here, the Supreme Court held that allowing such uncontrolled access without sufficient safeguards was an unjustifiable violation of citizens’ right to privacy.³⁴ Lastly, in the Indian Aadhaar case, the Supreme Court insisted on the application of judicial oversight to disclosure access.³⁵

Accountability and Grievance Redressal

A digital ID holder may come across any number of grievances while accessing their eFaas account, from being unable to register their account, to the collection of inaccurate information, to authentication errors that prevent them from accessing services. It is always crucial that accountability for such errors rests with authorities, and users are given appropriate recourse mechanisms to redress their concerns.

Concerningly, the eFaas policy fails to institute any grievance redressal systems. The policy also exempts the NCIT from expressly taking accountability for any errors or losses arising from the use of eFaas:


“The NCIT will not be liable for any loss or damage (including special, indirect or consequential) arising from or in connection with any of those elements of the eFaas system or its or their availability, use or performance either directly or through a third-party provider.”

This is a matter of concern; without proper accountability and grievance redress mechanisms, and considering the eFaas platform's control over access to crucial

³³ [Julian J. Robinson v. The Attorney General of Jamaica](#), [2019] JMFC Full 04, ¶ 367.

³⁴ [Madhewoo M v. The State of Mauritius](#), 2015 SCJ 177, 34; Centre for Internet and Society (2020). [Judicial Trends: How Courts Look at Digital ID Programs](#).

³⁵ *Ibid*, n. 29.



government services, individuals holding the ID may endure privacy violations and exclusionary harms stemming from the use of the ID system.


Data Protection Law

As much as the privacy policy sets out the rights and obligations of the ID holder and the administrator of the system (the NCIT), it cannot compensate for several important safeguards that only a data protection law can provide. Currently, there is no data protection law in the Maldives. Critically, this law would:

- Provide guidance to data controllers, processors and data subjects about the proper collection and processing of personal and sensitive personal data,
- Appoint a data protection authority charged with ensuring the compliant processing of data by both state and non-state entities, including the NCIT
- Provide data subjects with exercisable rights, including the right to consent to the processing of data, amongst others
- Require the NCIT to appointment a data protection officer who would oversee the actions of the NCIT or any third-party actor using the system in any way. Without a data protection officer, there is limited accountability within the NCIT, particularly when it is considered that the NCIT is performing really important functions of storing sensitive personal information and allowing access to important government functions to both state and private entities.

Conclusion and Recommendations

Currently, the digital applications of the national ID are not accounted for in the governing national ID law. This is dangerous, as all the issues arising from the use and misuse of the digital ID are left vague and unregulated. A comprehensive rule of framework is a necessary step before operationalizing a biometric digital ID system.



Recent updates in the country's digital ID policy – particularly with the World Bank's involvement – indicate a shift to a government-issued unique digital ID credential that will combine several functional identities, and possibly become necessary to access government services. The ongoing policy and infrastructural changes to the ID system must prioritize increasing trust in the digital ID system.

Recommendations

We urge legislators in the Maldives to:

- Implement a set of laws and policies governing the ID program, data privacy in the country, and cybersecurity and disaster management. This should cover all aspects of the digital ID system, the actors that may in any way interact with the system, grievance redress mechanisms, rights and duties of data subjects and the administrator of the system, amongst others.
- Enact a national data protection law to govern the processing of personal data in the Maldives, and ensure its applicability to the eFaas and any planned digital ID systems.

We urge the government in the Maldives to:

- Review the legal basis for the relationship with third-party private vendors to ensure that the collection and use of citizens' biometric data is well-protected. This required implementing additional measures beyond the contractual agreement to ensure accountability in the event of misuse.
- Create alternative forms of identity proof, to avoid creating an unnecessary dependence on one form of identity credential, which has the potential to cause an enormous exclusionary impact.



DIGITAL ID IN NEPAL

Summary

The *Nepāl Adhirājya's* (Kingdom of Nepal or Nepal) national, digital identity (ID) document enables access to various government and private services, including registering births and deaths, changing addresses, and purchasing mobile SIM cards. While becoming crucial for citizen interactions with the government, mandating the digital ID should be deferred until universal coverage is achieved and sustained. Further, alternative modes of proving identity should be allowed even after universal coverage is attained to reduce the exclusionary impacts of the ID system. To ensure inclusivity, the state should implement special arrangements for certain populations, including designating “introducers” to register individuals lacking ID documents, employing mobile initiatives, or subsidizing registration fees to increase registration, particularly for those facing barriers to accessing registration centers.

Historical Context

The registration of vital events – births, deaths, marriages, divorces, and internal migrations – has been ongoing in Nepal since 1976, with people registering their information at municipal committees and ward offices.¹ The Constitution of Nepal guarantees that every child has the right to name and birth registration.² Ensuring this right is the National Identity Card and Registration Act, 2020, which replaced the Births, Deaths and Other Personal Events (BDOPE, Registration) Act. The BDOPE Registration Act was enacted in 1977 and subsequently amended in 1980, 1991, and 2006.³

In 2018, the government officially launched its electronic national ID card program. The National ID card is a federal-level, chip-enabled, digital ID card that holds the personal and biometric data of the ID holder including the name, birth date, sex, photo, prints of all fingers and digital signature on a computer chip. These cards also contain unique identification numbers (National ID number) that are assigned to each newborn during birth registration, or when the person applies for a national ID card. The National ID Number is used to link personal records in the national ID database and the civil registration system. As of September 2022, the Department of National ID and Civil Registration reported that 120,000 cards have been distributed across Nepal, and over 700,000 have been printed.⁴

¹ Centre of Excellence for CRVS Systems (2020). [Country Profile for Nepal](#).

² [The Constitution of Nepal](#) (2015).

³ [Birth, Death and Other Personal Events \(BDOPE, Registration\) Act](#) (1976).

⁴ Kathmandu Post (2022). [A legion of safety concerns surrounds National ID scheme](#)

Identification Systems and Policies

National Identity Card and Civil Registration Act, 2020

The national ID system is governed by the National Identity Card and Civil Registration Act, 2020 (Nepal Identity Act).⁵ The Director General of the Department of National Identity Card and Civil Registration is tasked with implementing this Act and operationalizing the identity system.⁶ The Nepal Identity Act, among other things, regulates the integration of biometric identifiers into the national ID database.

The National ID Card Management (NIDMC) procedure under the Nepal Identity Act states that the national ID document will be the primary basis for obtaining all social services and “some private services”, although the latter services are not specified.⁷ Further, Section 34 of the Nepal Identity Act provides that various government bodies can have access to the biometric data collected by NIDMC, and even allows some level of access to the “agencies providing services.” The current system does not detail what safeguards are in place to protect citizens’ personally identifiable and sensitive data.⁸

The Nepal Identity Act further provides that only people with pre-existing “citizenship documents” are able to enroll in the national ID database,⁹ and sets out a separate ID system for Non-Resident Nepali (NRN) and Foreigners staying in Nepal for a period of time. In 2019, 77% of total births in the country were registered, and research shows some level of bias towards registering male compared to female children, though such bias has gone down significantly.¹⁰

⁵ Government of Nepal (2020). [National Identity Card and Civil Registration Act, 2020](#).

⁶ Ministry of Home Affairs, [Department of National Identity Card and Civil Registration](#).

⁷ Himal SouthAsian (2022). [Nepal’s biometric future](#).

⁸ Nepal Live Today (2023). [National ID Card System: A misguided priority](#).

⁹ UNFPA (2023). [Child Marriage and Gender-Biased Sex Selection](#); Biometric Future Identification Nepal (2022), *op. cit.*

¹⁰ Sharad K. Sharma et al., (2023). [Birth registration in Nepal: An assessment of progress based on two national surveys](#).

Data Protection Law

Nepal does not have a ‘unified data protection law’, with two laws currently serving to give effect to the right to privacy under the Constitution of Nepal. These include the Data Act 2079 (2022) and the Individual Privacy Act 2075 (2018) (‘the Privacy Act’).¹¹

Involvement of the World Bank

In June 2022, the World Bank approved a USD 180 million loan under an agreement with the Nepal Telecommunications Authority (NTA) for the implementation of the ‘Digital Nepal Acceleration (DNA) Project.’ This project will be implemented by the NTA, the Ministry of Communication and Information Technology, the Department of Information Technology, and the National Information Technology Center.

While this project does not directly fund digital identification efforts in the country, it does provide the government with support to ‘enhance the foundations for digital government... including enhancing the personal data protection regulatory framework.’¹² These efforts will directly impact Nepal’s identification ecosystem, including addressing the data protection concerns outlined below.

Implications of Nepal’s National ID System


Data Collection and Storage

Data minimisation is the practice of limiting the collection of personal information to that which is necessary to accomplish a specified purpose.¹³ Since a digital ID system essentially runs on citizens’ personal data, and often includes sensitive data such as biometrics, the principle of data minimisation must be strictly adhered to. In the absence of appropriate limitations on the data that can be legally collected, the ID

¹¹ Government of Nepal: The [Data Act](#) (2022) and the [Individual Privacy Act](#) (2018).

¹² The World Bank (2022). [Digital Nepal Acceleration \(DNA\) Project \(P176543\) - Project Information Document](#), Component 3.

¹³ ISACA (2021). [Data Minimization—A Practical Approach](#)



system is incentivised to collect as much data as possible to ensure convenience in case there is a future expansion of the ID system's scope or purposes.

Under the Nepal Identity Act, all Nepali citizens are eligible to receive the national ID card,¹⁴ and are required to apply for their ID card within two years of turning 16 years of age or within two years of the implementation of the system if they are already over 16.¹⁵ The data collected includes both personal information and biometric information. Personal information is defined to include “first name, last name, address, sex, date of birth, names of father, mother, spouse, and grandparents,” and also data relating to the applicant’s “qualification, occupation, profession, income, ownership maintained at any office or agency of the Government of Nepal.”¹⁶ The biometric information collected under the Act includes “digital image, fingerprints of ten fingers of both hands, iris scan of eyes, signature and other specified biometrics information of the applicant.”¹⁷

The Nepal Identity Act also specifies that the following information is recorded in the electronic database, for each person, including (a) first name, last name, (b) date of birth, (c) sex, (d) nationality, (e) national identity number, (f) date of issuing the NID and issuing authority, (g) photo, (h) address (permanent and temporary), (i) type of citizenship and citizenship number (for the person having citizenship), (j) biometric information, (k) name of parents, (l) name of grandparents, (m) name of spouse, (n) other information as specified.¹⁸

Notably, this is a vast dataset detailing copious amounts of information about every Nepali citizen. Due to the fact this is essentially an extension of Nepal’s civil


¹⁴ *Ibid*, n. 5, Section 4.

¹⁵ *Ibid*, n. 5, Sections 5 and 7.

¹⁶ *Ibid*, n. 5, Section 2(o).

¹⁷ *Ibid*, n. 5, Section 7.

¹⁸ *Ibid*, n. 5, Section 11.



registration system, such a wide collection of data is to be expected. However, the linkage of the ID and the civil registration datasets, along with the indefinite storage of all data in an electronic database,¹⁹ are major causes for concern. Additionally, all Nepali citizens are required to report personal events such as marriage, migration, divorce, death, amongst others, which will also be stored in the database.²⁰ Based on the foregoing, it cannot be argued that the principles of data minimisation are being followed under the Nepal Identity Act.

Additionally, this electronic database will also be linked to different government databases and offices.²¹ Concerningly, no additional information is provided about the specific government agencies that will be linked to the database, and there are no explanations provided regarding the controls governing data access or processing. Similarly, the Nepal Identity Act allows access to the Department of National Identity Card and Civil Registration to use any personal or biometric data that has been collected by any other government department under any other law.²² The governing law leaves the regulation of this system and the access of other agencies to the Government of Nepal to be prescribed in detail seemingly through rules, regulations, or notifications.

While it may be challenging to include comprehensive details about an ID system in the governing law, it is acknowledged that certain overarching rules should be established through the primary, rather than secondary, legislation. This would ensure a more concrete legal framework and safeguard against mission/function creep resulting from changes in governments or intentions.²³


¹⁹ *Ibid*, n. 5, Section 20.

²⁰ *Ibid*, n. 5, Sections 30 and 31.

²¹ *Ibid*, n. 5, Section 30.

²² *Ibid*, n. 5, Section 31.

²³ Electronic Frontier Foundation (2020). [Mandatory National IDs and Biometric Databases](#).



Moreover, the interconnection of these government databases and the unrestricted sharing of data with both state and non-state entities both have the potential to heighten the risk of unauthorized access and surveillance for data subjects in Nepal. This is due to the ease with which various databases can be compromised.²⁴ This concern is framed against a history of important government websites being hacked in Nepal, amplifying the urgency of the risk. Illustratively, 58 government websites were hacked, in one of the biggest computer systems breaches targeting a government, by a group called “Paradox CyberGhost.”²⁵


Purpose Limitation

Generally, the purpose limitation restricts the use of a digital ID system to certain legislative or regulatory uses. This is considered an important principle of data protection for biometric ID systems to comply with, as it dictates the scope and type of information that is collected from users, and the access different actors have to the system, among other key considerations. For instance, the Aadhaar biometric system in India was intended as a way for people to access government social schemes to identify themselves, allegedly to address fraudulent transactions that were occurring in welfare programs. As a result, the Aadhaar ID was only made mandatory to access these social schemes, data collected and stored correlated with those necessary to determine eligibility and only public agencies were allowed to access the system.

The Nepali ID system does not seem to include any purpose limitations and is generally a purpose-agnostic system, i.e., the system can be applied or utilized for various purposes without being restricted to a specific function or objective. Although not specified anywhere, its aim is directed towards having an extensive and accurate

²⁴ This was recognised by the High Court of Kenya in *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 882.

²⁵ The Kathmandu Post (2017). [58 govt websites ‘hacked to test vulnerability.’](#)



electronic record of every citizen, that can then be put to whatever use the government deems fit.


Exclusion

The prevalent challenge faced by digital ID systems worldwide is the exclusion of a certain portion of the population from accessing the ID platform, thereby limiting their access to the associated services. This is especially true for the migrant or undocumented population, disadvantaged communities, or those suffering from disabilities and infirmities.²⁶ This is not unexpected, as the introduction of an entirely new form of identity that is then made mandatory for access to public and/or private services can exacerbate the exclusion of at-risk populations. These systems have to be designed and implemented with special measures to include such populations at every stage of the ID program.

The Nepali ID system issues IDs only to Nepali citizens, therefore making proof of citizenship mandatory to obtain the ID. It even goes so far as to include as grounds for cancellation a “foreign individual” obtaining the card or if “the person who has obtained the card is no longer a Nepali citizen.”²⁷ Sections 4 and 9(4) of the Nepal Identity Act mentions that individuals who are eligible to obtain citizenship but have yet to obtain this are also eligible for the NID. In practice, however, this provision has not been implemented and the submission of a citizenship certificate remains mandatory when applying for the NID. This indicates that while policymakers may have the intention to include other residents or migrants who have yet to obtain citizenship, implementers have not paid attention to this aspect.

²⁶ Center for Human Rights and Global Justice, Initiative for Social and Economic Rights & Unwanted Witness (2021). [Chased Away and Left to Die: How a National Security Approach to Uganda’s National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons](#).

²⁷ *Ibid*, n. 5, Section 13.



However, this brings to the fore one of the core problems with digital ID policy that is aimed at inclusion and providing legal identity to the “undocumented”: when it relies on documentary proof to obtain the ID in the first place, it remains accessible only to those who already had a reliable legal identity.

According to a 2014 report by the Forum for Women, Law and Development,²⁸ *“possession of citizenship documents is significantly associated with gender and caste at the individual level, as well as with intra-family dynamics at the household level.”* Women in Nepal are far less likely to hold citizenship documents than men, and differences are also seen among castes and religions, with persons from the Chepang and Musahar communities and Muslims lagging behind their peers in citizenship acquisition rates. It was estimated in 2018 that over five million people do not have citizenship documents.²⁹


With this context, the government of Nepal must offer other means of acquiring the national ID, or take other special measures to include individuals and communities who are marginalized. For instance, under the Aadhaar system in India, persons who do not possess documents to prove their identity or address can be registered through a pre-designated “Introducer,” who is registered with the ID authority and vouches for the identity of the applicant.³⁰

Although this is something that can be implemented by the government while completing the registration and onboarding process, the ID law should specifically task the government with the responsibility of enacting these special measures, so that there are systems of accountability in place. It has been reported by bureaucrats

²⁸ Forum for Women, Law and Development (2014). [Acquisition Of Citizenship Certificate In Nepal: Understanding Trends, Barriers And Impacts](#).

²⁹ *Ibid*, n. 7.

³⁰ It is noteworthy that this system was not highly utilized with reports showing that less than 1% of Aadhaar ID holders were registered relying on this alternative measure.



that the national ID card will be the basis for all state-citizen transactions, and it is crucial to ensure persons who are already marginalized in society are not further isolated through this system.³¹

Disclosures Permitted by the ID System

Information collected through digital ID systems is often allowed to be disclosed to public authorities on grounds of national security, prevention of crime, compliance with judicial orders, amongst others.³² The governing law allows this through broad and vague provisions with limited oversight, such as “for the prevention or detection of crime”,³³ or “in the interest of national security,”³⁴ which in turn severely infringes ID holders’ privacy and autonomy rights (particularly since ID holders are not aware of the disclosure of their information).

Section 33 of the Nepal Identity Act stipulates that all the biometric and personal data in the database is confidential, except for reasons to do with verifying, deduplicating, or identifying the details of ID holders, as follows:

- a. if requested by an authorised officer in accordance with prevailing law for the investigation and prosecution of an offense,
- b. if the court so requires, or
- c. if requested by the concerned person.


There are no controls in place for this process, and the Nepal Identity Act does not ascribe liability to any person or authority in case of misuse of this disclosure system. Notably, there is also no requirement for ID holders to be notified that their data is

³¹ *Ibid*, n. 7.

³² Centre for Internet and Society, India (2020). [Judicial Trends: How Courts Look at Digital ID Programs](#), pp. 18-20.

³³ Section 43 of Jamaica’s National Identification and Registration Act, 2017. This provision was struck down in [Julian J. Robinson v. The Attorney General of Jamaica](#) [2019] JMFC Full 04, ¶ 367.

³⁴ Section 45, Data Protection Act, 2017 (Mauritius); Section 33, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (India).



being shared with law enforcement, and no mechanism for ID holders to appeal the decision. Typically, persons of interest have the right to post-surveillance notification that facilitates individuals to exercise their right to legal redress where their right to privacy has been violated.³⁵ Notably, allowing broad and unfettered access to a civilian information system that is otherwise connected to the day-to-day life of a citizen can pose a grave violation of their privacy, and where post-surveillance notification is not provided, this can thwart the right to legal redress and the right to privacy.

Recourse Mechanism

A digital ID law should have a well-designed and accessible grievance redress framework that addresses concerns of accountability, transparency, and user-friendliness. The Nepal Identity Act does not create an independent recourse mechanism for digital ID issues, but establishes the district court as the adjudicating authority for any cases arising from the Nepal Identity Act. It is unclear whether this jurisdiction applies only to the offenses created by the law, or to issues of authentication errors or failure to register persons, amongst others.

In any case, this is not a very accessible recourse mechanism, as it makes it infinitely harder for an ID holder or Nepali citizen to have their grievances addressed by going through a regular court system. When considering the range of problems that can arise in the operation of an ID system for a user, from omission or deactivation of the digital ID due to the provision of false information or non-use, to errors in the enrolment and verification process, or when there are authentication failures,³⁶ it is very important to set aside a specific and efficient recourse and appeal mechanism for ID holders to access.

³⁵ *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* [2021] ZACC 3.

³⁶ Centre for Internet and Society, India (2020). [Governing ID: A Framework for Evaluation of Digital Identity](#).

Conclusion and Recommendations

In Nepal, the national digital ID, allows access to government and private services and is envisioned to be the basis for registering births and deaths, changing addresses, and even buying a mobile SIM card. Inevitably, it will become crucial for citizens to have a digital ID for any interaction with the government. Where no alternative measures for identity proof are provided and where universal coverage has not yet been attained, this can result in the exclusion of citizens from the system, effectively preventing a segment of the population from accessing basic services.

Recommendations

We urge the government of Nepal to:

- Refrain from making the national ID a mandatory document in a citizen's life at least until universal coverage is achieved and maintained. Even then, the government should allow alternative modes of proving identity, which will support the reduction of exclusionary impacts.

We urge legislators in Nepal to:

- Amend the Nepal Identity Act and specifically task the government with the responsibility of implementing special arrangements for the registration of certain populations.

We urge the Department of National Identity Card and Civil Registration to:

- Adopt special measures to increase registration. This can include:
 - Deploying mobile initiatives to issue digital IDs to those who would otherwise struggle to go to registration centers, or
 - Offering subsidized registration fees for certain communities, among other measures.



DIGITAL ID POLICIES AND PRACTICES IN THE PHILIPPINES

Summary


The Philippine Identification System (PhilSys) is a fully functional biometric digital ID system established in a relatively short period, with the first step of registration commencing in October 2020.¹ The Philippine Identification Act (Republic Act No. 11055)² and the Philippine Data Privacy Act (Republic Act No. 10173)³ provide the guiding legal frameworks to support the roll-out of PhilSys and address concerns associated with the widespread digital ID system.

However, risks and potential misuse persist, necessitating ongoing efforts to mitigate adverse effects to individuals, including citizens and resident foreigners. One notable gap is the absence of an effective grievance redress mechanism, which could lead to increased exclusionary impacts and hinder ID holders in resolving everyday issues related to obtaining or accessing their digital ID.

¹ Philippine Statistics Authority (2020). [Step 1 of PhilSys registration to start on 12 October in 32 provinces.](#)

² The Philippine Identification Act (2018), [Republic Act No.11055.](#)

³ The Philippine Data Privacy Act (2012), [Republic Act No. 10173.](#)



Implementing a dedicated recourse mechanism that ensures accountability for unauthorized data sharing or discriminatory use of the ID system, while enabling direct complaints from ID holders without court intervention, would be beneficial. However, this should not bar individuals from seeking legal recourse through the courts, where they are aggrieved with the decision of the grievance redressal mechanism.

Moreover, the role of the data privacy law in enhancing security, transparency, and accountability in the digital ID policy is significant. Currently, the Philippine data privacy law is well-positioned to address privacy concerns related to the PhilSys system, which collects demographic and biometric information, but its applicability requires definitive clarification from the government or a court of law to avoid ambiguity in the legal governing framework.


Historical Context

One of the earliest attempts at a unified national ID system in the Philippines came with President Ferdinand Marcos signing Presidential Decree No. 278, which called for a National Reference Card System and the creation of a National Registration Coordinating Committee.⁴ It aimed to replace all existing government ID schemes with a single National Reference Card for Filipinos and resident foreigners.

Before the passage of the Philippine Identification System Act in 2018, other attempts at a national ID (and even a digital ID) did not materialize, with one attempt being struck down by the Supreme Court for violations of privacy rights.⁵ In 1996, President Fidel V. Ramos tried to introduce a computerized national ID system with biometrics to increase the ease of accessing government services and reduce fraudulent

⁴ Official Gazette (1973). [Presidential Decree No. 278, s. 1973](#).

⁵ Inquirer.Net (2017). [Controversial national ID system](#).



transactions.⁶ However, it was struck down by the Supreme Court, with Justice Reynato Puno contending that the national ID system “will put our people’s right to privacy in clear and present danger” and the “vast reservoir of personal information [collected in the ID] constitutes a covert invitation to misuse, a temptation that may be just too great for some of our authorities to resist.”⁷

In 2005, through another Executive Order, President Gloria Macapagal Arroyo called for a system that consolidates different existing government identification systems. This led to the Unified Multi-Purpose ID system in 2010. This Order was also challenged in court, but the Supreme Court upheld its constitutionality, because the data points collected by this system were limited, and did not include any additional data collection that was not already part of existing government ID schemes.⁸

The Philippines’ first attempt at creating a digital ID system came in 2018, when after a series of Senate bills,⁹ the Philippine Identification System Act was passed. This Act required the government to create a single official identification card for all citizens and foreign residents that would serve as a *de facto* national identification number. Aside from acting as official proof of identity, the PhilID would allow access to a wide range of public and private services.¹⁰

The rationale for the PhilID’s classification as a digital ID is the ability for ID holders to be identified, verified and authenticated digitally during online transactions. As of May 30, 2023, 65 million PhilIDs were printed and dispatched.¹¹

⁶ Rappler IQ (2018). [Past attempts at a national ID system: A battleground of privacy, executive power.](#)

⁷ *Ibid.*, n. 5.

⁸ Supreme Court Manila (2006). [Kilusang Mayo Uno & 6 Ors. vs The Director-General, National Economic Development Authority & the Secretary, Department of Budget and Management](#), G.R. No. 167798.

⁹ Senate Bill No. 1500 filed on July 18, 2017, Senate Bill No. 1510 filed on July 25, 2017, Senate Bill No. 1577 filed on September 4, 2017, and Senate Bill No. 1579 filed on September 6, 2017.

¹⁰ Republic of the Philippines - Philippine Identification System. [PhilSys Use Cases.](#)

¹¹ Republic of the Philippines - Philippine Identification System (2023). [65M PhilID and ePhilID issuance reached.](#)

Involvement of the World Bank

In December 2021, the Philippine government secured a USD 600 million loan from the World Bank, part of which was to be used for the development of the Philippine Identification System. The project, dubbed ‘Philippines Promoting Competitiveness and Enhancing Resilience to Natural Disasters Sub-Program 3 Development Policy Loan’¹² is expected to:

“...increase access to and improve delivery of public services by providing Filipinos with a unique, verifiable digital identity... Filipinos can use this foundational ID for key public and private transactions, including opening bank accounts, identifying, and verifying social assistance beneficiaries, and making pension payments by 2022.”¹³

Philippine Identification System


The Philippine ID system has the following components: the PhilSys Number (PSN), the PhilID, and the PhilSys Registry.

1. The **PSN** is a unique and randomly-generated 12-digit permanent identification number assigned to every citizen or resident alien upon successful registration to PhilSys. On the PhilID, the PSN is tokenized as the PhilSys Card Number or PCN to protect against misuse and identity fraud.¹⁴ The PSN itself is highly confidential, and ID holders are encouraged to only share their PCN for online and physical transactions.
2. The **PhilID** is a non-transferable card containing the ID holder’s demographic and biometric information such as full name, birth date, address, front-facing photograph, and PCN. The back of the PhilID is a micro-printed version of the

¹² World Bank (2021). [Press Release - World Bank Approves New Project to Support Competitive and Resilient Recovery in the Philippines](#).

¹³ *Ibid.*

¹⁴ Republic of the Philippines - Philippine Identification System. [PhilSys Number](#).



PSN, along with the date of issuance, gender, blood type, marital status, place of birth, and a digitally-signed QR code.¹⁵

3. The **PhilSys registry** is the database that contains all registered information of ID holders, including PSNs, all application form information, and any updates made by ID holders.¹⁶ It is owned, maintained, and administered by the Philippine Statistical Authority (PSA).¹⁷

Implications of the Philippine Identification System

Like any other government policy, the success of a digital ID system must be measured against its purposes or objectives. Generally, the conceptualization and deployment of digital ID systems comes with enormous costs, both monetary and human-rights related, and any examination of its impact must begin with its stated purposes or objectives, i.e., the gap that made the digital ID system necessary.

Objectives

According to the Philippine Identification System Act, the objectives of the PhilID are:¹⁸


1. To establish a single identification system for citizens and residents
2. To provide valid proof of identity to simplify public and private transactions
3. To eliminate the need of having different identifications when transacting with government and private services

¹⁵ *Ibid.*

¹⁶ *Ibid.*

¹⁷ Republic of the Philippines. [Philippine Statistics Authority](#).

¹⁸ *Ibid.*, n.2, Section 3.

- 
4. To act as a social and economic platform for services and strengthen financial inclusion
 5. To enhance administrative governance, reduce corruption, and promote ease of doing business.

Information Collection and Storage

Data minimization is an integral principle of the protection of personal data, and its practice requires limiting the collection of personal and sensitive personal information to that which is necessary to accomplish a specific purpose.¹⁹ Since a digital ID system requires, and essentially runs on, the collection and processing of individuals' personal data, including sensitive data like biometrics, the principle of data minimization must be strictly followed.

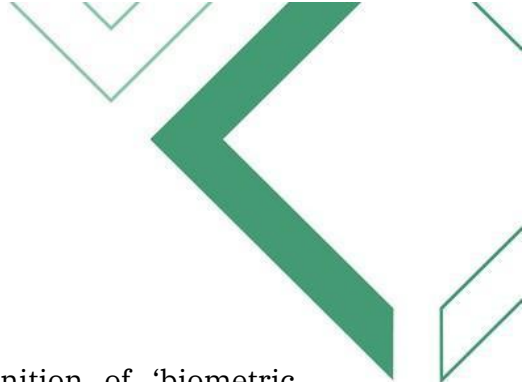
The PhilSys system collects both demographic and biometric information. Demographic information includes data about ID holders' name, sex, age, address, place of birth, address, nationality status, blood type, etc. Biometric information includes photographs, a full set of fingerprints, and iris scans.²⁰

Relative to many other digital ID systems in other parts of the world, the PhilSys collects a limited set of data, without many data points that could identify a discriminated community or person. Additionally, both Section 8 and the definitions of personal and biometric data in Section 5 of the Philippine Identification Act, leave no room for the government or the PSA to add any more data points (to collect from ID applicants) without legislating it into this Act.

This is a common problem, where the governing act is vague and allows many significant changes to be brought in easily through executive functions.

¹⁹ Ministry of Electronics and Information Technology (2018). [White Paper of the Committee of Experts on a Data Protection Framework for India](#).

²⁰ *Ibid*, n. 2, Section 8.



Comparatively, the Aadhaar Act in India allows the definition of ‘biometric information’ to extend to “any other information that may be specified through regulation.”²¹ This allows the executive government to easily change the amount of data that can be collected through the Aadhaar Act, without it having to go through legislative processes.²²

Concerningly, neither the Philippine Identification Act nor the PSA’s Privacy Policy, which was developed in accordance with the Data Privacy Act (2012) reveals how long the collected data will be retained. This is of concern noting that authentication records can detail an ID holder’s transactions using the PhilID, and who the relying party was.

Typically, data subjects’ right to erase or amend their data underpins personal data protection and privacy laws. While Section 11 of the Philippine Identification Act permits ID holders to update their registration information, no similar provision is expressly provided for ID holders to delete or erase their data records from PhilSys, even when their ID has been deactivated.²³ Additionally, the Data Privacy Act does not provide clarity on this right, which challenge is further compounded by National Privacy Commission (NPC)’s Advisory Opinion that ID holders/applicants do not have a right to erasure under the Data Privacy Act.²⁴

²¹ Section 2(k), [Aadhaar Act](#).

²² The Centre for Internet & Society, India (2020). [Governing ID: India’s Unique Identity Programme](#).

²³ *Ibid*, n. 2, Section 9.

²⁴ National Privacy Commission (2022). [Advisory Opinion No.2022-018](#).

Public and Private Actors

PhilSys does not impose any restrictions on actors that can use or access the system, as relying parties. Both private and government entities can use PhilSys for authenticating the identity of the ID holder. The relying party is expected to conform to standards and guidelines set up by PSA to ensure the security, efficiency and integrity of the authentication process, but apart from that, there are no other restrictions that limit or control on private agencies unlimited access to the PhilSys.²⁵

The process of authentication involves sharing demographic information, biometric information, one-time passwords (OTP) or PSN/PhilID with the relying party, who will, in turn, share it with the PSA to validate the ID holder's identity.²⁶ The PSA can respond to the relying party with a 'Yes/No' answer but is also allowed to share the ID holder's demographic information or photographs, depending on the use case.²⁷ The Act does put in place some controls for this data sharing – the ID holder must be informed specifically of the data that will be collected and for what purpose it will be used; the relying party is proscribed from using it for any other purposes.²⁸ It is however important to note that the use of the national ID system by private parties is often considered a privacy risk that permits the commercial exploitation of ID holders' biometric information by private companies.²⁹

²⁵ *Ibid*, n.2, Section 12.

²⁶ *Ibid*, n.2, Section 12.

²⁷ *Ibid*, n.2, Section 12.

²⁸ *Ibid*, n.2, Section 12.

²⁹ Section 57 of the Aadhaar Act, which permitted private parties to seek authentication on the basis of a contract, was struck down by the Supreme Court of India, as it allowed commercial exploitation of Aadhaar holders' privacy in *Aadhaar judgement*, para 513.8.3



Privacy

Section 8 of the Philippine Identification Act makes it mandatory for all citizens and resident aliens to register for the PhilID. The PhilID is intended to be the official government ID in the Philippines, replacing existing IDs from different government agencies. To that end, Section 24 of the Philippine Identification Act tasks the PSA with transitioning existing government identification schemes into the PhilSys through seeding of the PSN and consolidation of platforms. However, the right to identity does not equate to making identification a mandatory requirement for citizens or residents.


The mandatory collection of biometric information of citizens and resident foreigners has been challenged in courts across the world in recognition of the privacy and security risks, typically with success.³⁰ This report recognises that the data collection requirements for physical and digital ID systems vary significantly, and reiterates that the privacy and security risks of the latter system far outweigh those of a regular card-based identity system. In addition to the collection of biometric data, each instance of authentication of the digital ID by users leads to the creation and storage of more personal data. This results in a vast collection of personal and sensitive personal data on every citizen or resident of the Philippines which is accessible to several state and non-state actors without adequate safeguards through the PhilSys.

The impact of this can also be seen through the NPC³¹ Advisory Opinion issued in September 2022.³² When asked about the rights of a person registered in the PhilSys as a data subject under the Data Privacy Act, 2012, the privacy commission stated that consent is not the basis of processing personal data under PhilSys, but a legal

³⁰ The Centre for Internet and Society (2020). [Judicial Trends: How Courts Look at Digital ID Programs](#), p. 17.

³¹ The National Privacy Commission is the administrator of the Data Privacy Act, 2012 that also acts as an advisory body on matters of personal data protection.

³² *Ibid*, n. 22.



obligation. As a result, the registered person does not have the same rights of withdrawal of consent as a data subject under the Data Privacy Act.³³

Similarly, a person registered in the system does not have the right to delete or erase their personal data from the PhilSys, as there is no express provision allowing it in the Philippine Identification System Act (although a person's PSN may be deactivated, their personal data will continue to remain in the system.) According to the NPC's advice, the absence of express provisions in the PhilSys law allowing for deletion in the system eliminates the registered person's right to erasure under the Data Privacy Act.³⁴ This is concerning, as the national data protection law should operate in addition to the biometric ID law to fill any gaps unaddressed by the latter. Removing the applicability of data protection provisions that were not *expressly* allowed by the ID governing law introduces risks, vulnerability, and unpredictability into the system.

Uses of the System and Risk of Surveillance


A purpose limitation restricts the use of a digital ID system to certain legislative or regulative uses, is integral to the processing of individuals personal data under both data protection and privacy laws. This is considered an important principle for biometric ID systems to comply with, as it can also set the scope of what kind of information is collected from users, the access different actors have to the system, amongst others.

In the case of PhilSys, the PhilID is intended to act simply as a mode of identity verification that can be used in any transactions that require proof of identity.³⁵ This ranges from eligibility for government social security schemes and voter

³³ *Ibid*, n. 22: "Since it is the law and not consent that is the basis for processing under the PhilSys, the right to withdraw consent by the data subject does not apply. There is no consent to speak of since the registration to PhilSys is a legal obligation imposed upon every citizen or resident alien."

³⁴ *Ibid*, n. 22.

³⁵ *Ibid*, n. 2, Section 14.



identification, to school applications and employment purposes, among others.³⁶ The vast purposes of the biometric ID put an ID holder at risk of surveillance, as the user's day-to-day life can be retraced simply based on where they authenticated their PhilID. The PhilSys stores the “Record History” of every ID holder, which includes the following details of their authentication requests: the date the request was made and processed, the relying party, and the response provided by PhilSys.³⁷ If the ID is used often and for different transactions or services, a clear record can be created to identify and profile the user. Along with the embedding of the PSA in different government identification systems and the centralized storage of this information, this can allow unscrupulous actors to profile users, track movements, assess their habits, and influence their behaviour.³⁸

The multiple uses associated with the PhilSys also have the added risk of creating a dependence on the system, in which PhilID starts to replace many different forms of ID to the extent that it is impossible to survive in the Philippines without having or using it. As seen in the case of India, despite the largely “voluntary” nature of the Aadhaar identity system, it has become a default proof of identity in India, with service providers refusing service unless citizens provide their Aadhaar card (despite laws that prohibit them from doing this).³⁹

Disclosure of Information


Information collected through digital ID systems is often allowed to be disclosed to public authorities for reasons associated with national security, prevention of crime, compliance with judicial orders, amongst other national, legal, or public interest

³⁶ *Ibid*, n. 2, Section 5: Registered information refers to any personal information regarding a citizen or resident alien recorded in the PhilSys, including biometric information and information about a citizen or resident alien required under this Act to be recorded under the PhilSys.

³⁷ *Ibid*, n. 2, Section 4(I).

³⁸ The Jamaican Supreme Court struck down their biometric digital ID system because of the risks of surveillance it posed, in *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 30, 375.

³⁹ Quartz (2018). [Aadhaar is voluntary—but millions of Indians are already trapped.](#)



purposes.⁴⁰ The governing law typically allows this through broad and vague provisions with limited oversight which in turn severely intrudes ID holders' privacy and bodily autonomy rights (particularly since ID holders are not aware of the disclosure of their information). A few examples of this include the Jamaican provision which permitted the disclosure of personal data in the digital ID database for “for the prevention or detection of crime”,⁴¹ or in the cases of Mauritius and India - “in the interest of national security.”⁴²

The Philippine Identification Act does not permit the disclosure of such information, even to law enforcement agents, except in the following two cases, (a) If the ID holder has consented specifically to this disclosure, or (b) through an order of a competent court, if a compelling interest of public health/safety with significant risk is established.⁴³ It also mandates the PSA to notify the owner of the information within 72 hours of such disclosure.

These safeguards are a positive and protective feature in the Philippine Identification Act, as they create necessary obstacles in the way of sharing personal information that was meant to be used only for the identification system, to third parties and for other purposes. Section 19 of the Act also imposes imprisonment and fines on officers who allow access to or otherwise share PhilSys data in contravention of the Philippine Identification Act.

⁴⁰ *Ibid*, n. 28, pp. 18-20.

⁴¹ Section 43, Jamaica Act (provision was struck down in *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 367).

⁴² Section 45, Data Protection Act, 2017 (Mauritius); Section 33, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (India).

⁴³ *Ibid*, n.2, Section 17.

Recourse Mechanism

There are several points in an ID holder's journey from registration and getting an ID, to using it in their day-to-day life, where issues may arise. This can range from data being inaccurately seeded into the system⁴⁴ to authentication errors while establishing identity during a transaction, to the unauthorized sharing of data with third parties. Since this ID is being used to access both state and private services, and the data collected includes both personal and sensitive personal data, it is very important to have accessible recourse mechanisms that ID holders or ID applicants can use to quickly address their grievances.


Notably, the Philippine Identification Act does *not* set up any recourse mechanism that ID holders can rely on to raise their grievances. The Data Privacy Act of 2012 does establish a recourse mechanism for data subjects whose data has been shared or accessed in contravention of the Act, this would only apply to privacy-related grievances that impact data subjects' rights.

Exclusion

Digital ID systems across the world have been notoriously controversial for their role in excluding segments of country's populations from accessing and using national ID platforms. This is especially true for migrant or undocumented populations, oppressed communities, or those suffering from disabilities and infirmities.⁴⁵ National efforts to introduce an entirely new form of identity, and then create bottlenecks to public services based on an accurate reading of this identity-proof, carries significant risks of excluding at-risk populations. To this end, digital ID

⁴⁴ PhilStar Global (2023). [Encoding errors plague national ID; PSA to conduct updating.](#)

⁴⁵ Center for Human Rights and Global Justice, Center for Human Rights and Global Justice and Unwanted Witness (2021). [Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons.](#)



systems have to be introduced with special measures to cater and provide protection for at-risk populations at every stage of the digital ID program.

Positively, we note that the PhilSys provides some of these protective measures, including:

1. It allows for “biometric exceptions” in case capturing biometric information during registration is impossible due to physical or visual impairment⁴⁶ (although there is no more detail on how this biometric exception works, or in what situations it may be allowed).
2. The PSA is required to issue guidelines for special arrangements to be made (by registration centres) for the registration of certain populations like senior citizens, persons with disabilities, indigenous persons, single parents, etc.⁴⁷
3. The PSA is tasked with ensuring that the registration process and the documents required to register are not prohibitive in any way. To that end, applicants who do not possess any of the necessary documents can be endorsed by a qualified “introducer” to vouch for their identity.⁴⁸ If this is implemented well, PhilSys could be successful in including those who previously did not have any reliable forms of government ID.
4. The PSA conducts mobile initiatives to issue digital IDs to those who would otherwise struggle to go to registration centers, such as street dwellers, vulnerable children, families, and indigenous peoples.⁴⁹

⁴⁶ *Ibid*, n. 2, Section 8.

⁴⁷ *Ibid*, n. 2, Section 9.

⁴⁸ *Ibid*, n. 2, Section 8(C)(4).

⁴⁹ Biometric Update (2023). [Philippines conducts biometric registration of vulnerable people, total hits 29M milestone.](#)




Conclusion and Recommendations

The Philippine Identification System is a fully functioning biometric ID system, conceptualized, designed and operationalized in a span of only five years (2018 - 2023). The Philippine Identification Act and the Data Privacy Act are both critical legal frameworks that will go a long way in assuaging some of the concerns introduced by a pervasive digital ID system. However, the potential for risk or misuse in the system is still large, and efforts need to continue to be made to minimize harm from the use of the system.

Recommendations

We urge the Philippines government to:

- Provide an effective and dedicated grievance redress mechanism for applicants or ID holders with digital ID-related issues. This recourse mechanism should also specifically introduce:
 - accountability measures for issues like unauthorized sharing of data, or discrimination in use of the ID system;
 - allow complaints to be made directly by ID holders without the intervention of a court. However, this should not bar individuals from seeking legal recourse through the courts, where they are aggrieved with the decision of the grievance redress mechanism.
- Clarify that the Philippine Data Privacy law governs all data collection and processing activities undertaken under the Philippine Identification Act. Specifically:


- 
- the National Privacy Commission's advisory opinion disputing the applicability of the Data Privacy law to the ID Act makes for a very vague and unpredictable legal governing framework, and should be reversed.

DIGITAL ID IN SRI LANKA

Summary

The electronic NIC (e-NIC) program in *Ilangai Jananayaka Socialisa Kudiarasu* (Sri Lanka or Democratic Socialist Republic of Sri Lanka or Ceylon or *Sri Lanka Prajatantrika Samajavadi Janarajaya*) is currently well regulated by the ID law and the newly-enacted Personal Data Protection Act, No. 9 as of 2022 ('PDPA'), although the impact of the latter is yet to be fully realized. However, there is a shift towards transforming the digital ID system from a digitized civil registration system to an independent digital identity (ID) platform similar to India's Aadhaar system. This transition aims to decentralize data storage and government control but may introduce challenges such as third-party access, authentication records, and real-time surveillance. The policy and governing framework must be designed in parallel with technological advancements to address potential risks comprehensively.

The current e-NIC is mandatory as it serves as the digitized version of the country's primary ID document. However, considering the significant privacy and exclusionary implications of a mandatory digital ID system, it is recommended to amend this policy and allow alternative modes of identity verification to promote inclusivity. To prevent



further marginalization, the new digital ID system should accommodate multiple registration methods beyond NIC or birth certificates.

Historical Context

Civil Registration and Vital Statistics System (CRVS)

Sri Lanka's civil registration system is governed by the Births and Deaths Registration Act, 1954.¹ It is a very well-developed system, with 97% of total births registered according to Demographic and Health Survey (DHS) data.² In 2009, the birth registration process was decentralized, and in 2017 it began being digitized.

Foundational Identity System

Sri Lanka has a long history of foundational ID provision, starting with the Registration of Persons Act No. 32 as of 1968.³ This system registers all Sri Lankan citizens aged 15 and above in a National Persons Registry and provides them with a national ID card (NIC). According to World Bank statistics, 95% of men and 90% of women in Sri Lanka own a national ID card.⁴ More recently, the government of Sri Lanka began digitizing the National Persons Registry and the NIC as part of a long-term plan to digitize Sri Lanka's foundational and functional ID systems.

Electronic NIC


The electronic NIC (e-NIC) project has been a long-time goal of the government, but it is yet to fully take effect. There is very limited publicly available information about the progress or operation of this system. However, according to the Department of Registration of Persons, the authority tasked with implementing all identity/registration-related processes in Sri Lanka, the e-NIC project aims to

¹ Blackhall Publishing. [Births and Deaths Registration Act](#), 1954.

² GSMA (2019). [Digital Identity Country Report: Sri Lanka](#).

³ LawNet Ministry of Justice. [Registration of Persons Act No. 32 of 1968](#).

⁴ World Bank Group (2018). [ID4D-Findex Survey Data 2018](#).



*“facilitate the general public to obtain their day-to-day services and facilitate national security and accelerated economic development of the country”.*⁵

Under this, the project aims to establish a national persons database with the biodata of persons 15 years old and above, containing biometrics in the form of fingerprints and photographs. This system does not yet support electronic authentication or have an identity platform to access services.

Identification Systems and Policies

The Registration of Persons Act (RPA), 1968, sets out the requirements and procedures for obtaining national ID cards. The RPA appoints a “Commissioner” along with Deputy and Assistant Commissioners to manage the national ID registry or database and discharge all the functions under the Act.⁶ Several amendments were made to this Act, twice in 1971 and then once in 1981, but most notable was its amendment in 2016, when provisions were made to introduce electronic and biometric features and convert the registry into a database.⁷ The RPA, regulations issued under it, and the PDPA, 2022, form the framework of laws that governs the e-NIC system.

Upcoming Policies: Unitary Digital ID Framework


In early 2022, the Sri Lankan government announced that it would obtain a grant from India to create a “Unitary Digital ID Framework” in the country. The grant is estimated at 300 million Indian rupees, or approximately USD 3.8 million.⁸ The scheme is intended to introduce a *“personal identity verification device based on biometric data, a digital tool that can represent the identities of individuals in cyberspace, and the identification*

⁵ Department of Registration of Persons. [e-NIC Project](#).

⁶ *Ibid*, n. 3, Sections 3-5.

⁷ Parliament of the Democratic Socialist Republic of Sri Lanka. [Registration of Persons \(Amendment\) Act No 8 of 2016](#).

⁸ Biometric Update (2022). [Sri Lanka digital ID contract bids open soon: only Indian firms need apply](#).



of individual identities that can be accurately verified in digital and physical environments by combining the two devices.”⁹ This model is based on the Aadhaar framework in India, and will offer an authentication platform to access government services,¹⁰ which is currently not available under the e-NIC program. This project is still underway, with very limited publicly available information.

Implications of Sri Lanka’s ID System

Mandatory Registration

Sections 2 and 8 of the RPA make it mandatory for all Sri Lankan citizens aged 15 years and above to register for the NIC. Failing to register or providing incorrect information during registration, is an offense that can invite a fine of up to 5,000 rupees (USD 15.5).¹¹ While the mandate for obtaining a national ID card may be justifiable since it forms an important citizenship document in Sri Lanka, the mandatory collection of biometric information is not.

Notably, the sharing and storing of important data like biometrics should always be based on consent and not legal liability. Recently, the Supreme Courts of Jamaica and Mauritius struck down their national biometric ID systems because they felt it was an unjustifiable violation of privacy to coerce citizens to share their biometric data with the state.¹²

⁹ Biometric Update (2022). [India to sign MoU to bring Sri Lanka its own digital identity system.](#)

¹⁰ The Register (2022). [Sri Lanka to adopt India’s Aadhaar digital identity scheme.](#)

¹¹ *Ibid*, n. 3, Section 44.

¹² The Centre for Internet and Society, India (2020). [Judicial Trends: How Courts Look at Digital ID Programs](#), p. 17.

Data Collection and Storage

Section 6 of the RPA (2016 amendment) delegates the responsibility of prescribing the data that will be collected and stored in the national registry to the executive government through regulations.¹³ While this is common in other digital ID systems around the world, it is still a concerning practice, because it permits the addition of new categories of data to be collected without undergoing the legislative process. Delegating this legislative function to the executive, through the issuance of regulations or notifications, can put citizens' privacy at risk, as it too easily allows the collection of more invasive data in a way that dilutes constitutional protections otherwise accorded to important citizen rights.


Section 6 of the RPA Regulations tasks the Commissioner to record the following information about each citizen in the national registry: (a) name, (b) date of birth, (c) place of birth, (d) gender, (e) address, (f) family details, and (g) numbers of the national ID cards of parents, guardian, spouse, children, and siblings.

Additionally, applicants have to provide the following details while submitting their application form:

1. Prescribed biometrics taken by the Commissioner-General or by a person authorized by him;
2. Photographs of the applicant of the prescribed dimensions, specifications, standards and quality;
3. Image of the applicant taken by the Commissioner-General or by a person authorized by him.

Since this is essentially the main ID and citizenship program in Sri Lanka, this would be the minimal amount of data the government could collect to achieve its objectives.

¹³ *Ibid*, n. 3, Section 6 (2016 amendment).



However, its linkage to an electronic database, particularly with the addition of biometrics can be concerning.

It is unclear from these policies exactly where the biometric data is stored, specifically, whether it is stored only on the e-NIC card or elsewhere. In any case, this database comprises sensitive personal data of nearly all the citizens of Sri Lanka and security risks and breaches are a grave concern. In addition to proper technological security measures, the database should be regulated by cyber security and disaster mitigation policies in case of data breaches or any other security crises.

Disclosure


Digital ID systems often allow disclosures of citizen information to public authorities without their consent, in certain situations. With the vast data that a digital ID system collects, this access, particularly for law and order or criminal investigation purposes, often forms an important part of digital ID policies.

Section 39 of the RPA Act allows the Commissioners to disclose information concerning the registered person under three circumstances:

1. In the interest of national security upon a direction issued by the secretary to the Ministry of the Minister to whom the subject of national defense is assigned;
2. For the prevention or detection of crimes; or
3. For the purpose of complying with any order or direction issued by a competent Court.¹⁴

While the permissible circumstances for disclosure are limited, they are very wide in scope and impose very few restrictions on what may be eligible under this section.

¹⁴ *Ibid*, n. 3, Section 39C.



“National security” and “prevention or detection of crimes” are very vague terms, typically without settled jurisprudence on what they entail. This is concerning, as it can directly impact the privacy rights of ID holders. There is no system of accountability for the unwarranted disclosure of citizen information prescribed in the RPA, and citizens have limited recourse to complain in case they believe their information was wrongly disclosed.

The scope and conditions for disclosure have been well debated before by courts around the world, for similar data-intensive digital ID systems. In Jamaica, when the Supreme Court was hearing a case on the constitutionality of their national digital ID system, the court held that vague terms used in the disclosure provision, such as “when authorized by law” or “for the detection and prevention of crime,” was an unconstitutional violation of ID holders’ privacy rights.¹⁵ Similarly, in Mauritius, disclosures from the digital ID system were allowed for reasons of national security and the prevention of crime in the absence of any judicial oversight; the Supreme Court there held that allowing such uncontrolled access without sufficient safeguards was an unjustifiable violation of citizens’ right to privacy.¹⁶ Even in the Indian Aadhaar case, the Supreme Court insisted on the application of judicial oversight to disclosure access.¹⁷

Grievance Redressal


The RPA sets up a Registration of Persons Tribunal where applicants can appeal the Commissioner’s decisions on “any application for registration, or for the duplicate of an identity card.”¹⁸ These tribunals may be set up in every district, but it is unclear how many have been already set up and are operational. The creation of an accessible

¹⁵ *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 367.

¹⁶ *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 34; Centre for Internet and Society (2020). [Judicial Trends: How Courts Look at Digital ID Programs](#).

¹⁷ *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 232, ¶ 144.

¹⁸ *Ibid*, n. 3, Sections 25 & 26.



tribunal that is devoted to hearing cases on the national identity card and database is a commendable and emulable move towards reducing the exclusionary impacts of this program and increasing the accountability of the administrator of the system.

Data Protection

In March 2022, the PDPA 2022 came into effect in Sri Lanka.¹⁹ The PDPA applies to all controllers and processors located in Sri Lanka who process the personal data of citizens and non-citizens for any commercial or non-commercial purposes.²⁰ The definition of ‘controller’ includes “public authority” and “public corporation,” and based on this, the PDPA 2022 applies to the collection of data under the e-NIC project.²¹

Once it comes into effect within 18–36 months, the PDPA 2022 will apply to the processing of all personal data, whereas the RPA does not offer the same comprehensive protection. This is promising, as it will fill any data protection gaps left by the RPA framework. The PDPA 2022 has not yet been properly enforced, but some noteworthy provisions that would make the e-NIC program more privacy-enhancing include:


1. **Data breach notifications:** The PDPA 2022 mandates that controllers notify data breaches to the authority and/or to the data subjects in such manner, form and within such time as may be determined by rules to be made under the law. The circumstances under which the data protection authority and/or data subjects must be notified are to be stipulated by the authority in due course.²²
2. **Data Protection Impact Assessment:** Controllers are expected to carry out data protection impact assessments to identify risks before carrying out

¹⁹ Parliament of the Democratic Socialist Republic of Sri Lanka. [Personal Data Protection Act, 2022](#).

²⁰ *Ibid*, Section 2.

²¹ *Ibid*, Section 56.

²² *Ibid*, Section 23.



certain types of processing activities, and where required, seek the opinion of the data protection authority.²³

3. **Data Protection Authority:** The PDPA 2022 establishes a data protection authority that will ensure compliance by entities with the law, conduct inquiries, hear grievances and appeals, and issue directives on entities which do not adhere to the provisions of the proposed law.²⁴ A data protection authority can hold the Commissioner (in the e-NIC system) and any other actor that accesses the e-NIC system or database in an unauthorized manner, accountable for their actions.


Conclusion and Recommendations

Currently, the e-NIC program is well regulated by a combination of the ID law and the newly-enacted PDPA 2022, the impact of which is yet to be felt. The e-NIC is currently mandatory – a consequence of it being a digitized version of the country’s most important ID document. However, the privacy and exclusionary impact of a mandatory digital ID system is large, especially if tied to eligibility for important government services.

Further, the Sri Lankan digital ID system seems to be moving from a digitized civil registration system to an independent digital ID platform, similar to India’s Aadhaar. In the move to an Aadhaar-like platform, several new features will (most likely) be added: the ability for a service provider to verify or authenticate the user’s identity entirely online; applications built atop the identity platform that will be used for online banking services, electronic Know-Your-Customer services; and the opening of the ID platform to private players.

²³ *Ibid*, Section 24.

²⁴ *Ibid*, Sections 28-32.



This will help decentralize the data stored in the system on every individual and will further decentralize the government's control. However, this decentralization may introduce other problems such as access by third parties, the creation of authentication records, and real-time surveillance, among others, which have not been accounted for in the current policy.

To ensure that all citizens or residents are accounted for in the new digital ID system, the law should account for more than one way to register for the digital ID. In the presence of a strong national ID system or database, it is most likely that those registered in the NIC system will be easily transferred to the new database. To ensure that there is no case of further isolation of those already excluded from the existing system, the new digital ID policy should allow more than one way (apart from just NIC or birth certificate) to register.

Recommendations

We urge the government of Sri Lanka to:

- Simultaneously adopt the policy and governing framework alongside the technological design – as opposed to coming after – to ensure that all possible harms of the system are carefully accounted for.

We urge legislators in Sri Lanka to:

- The e-NIC law should be amended to introduce and encourage alternative modes of identity registration and verification, beyond the NIC or birth certificate.

**EngageMedia.org/
Greater-Internet-
Freedom**