Putting People First in Sri Lanka’s Digital Public Infrastructure Push

This brief has been produced by Pamodi Waravita, June 2025

Introduction

Like many countries, Sri Lanka has been considering methods of utilising technology to improve its citizen services since the adoption of computers and the internet in the early 2000s. However, events like Covid-19 and the economic crisis, combined with the widespread adoption of smartphones and island wide internet connectivity, have ignited the agenda around Digital Public Infrastructure (DPI).

Sri Lanka’s economic crisis in 2022 left many devastating impacts in its wake, including the halt of essential services to the public like health, welfare, and education. These events followed closely on the heels of Covid-19’s lockdowns which also left people scrambling to find digital-based services to meet their essential needs. With both crises exemplifying the interdependent nature of the economy and public infrastructure/services, Sri Lankan policymakers have begun to seriously think about DPI in its economic recovery model.

From a digital rights perspective, DPI was originally envisioned as ‘civic tech’, more as a community-driven, decentralised infrastructure aimed at improving citizens’ engagement and interactions with government services, and participation in civic engagements through digital spaces. However, influential actors leading discussions at the international level have shifted this collective outlook of a ‘digital civics’ towards more transactional systems that focus on government service delivery and financial access, and on building pathways for private-sector growth, rather than supporting community-led innovation.

In defining DPI, players like the Gates Foundation name economic advancement as a primary objective:

"Digital public infrastructure (DPI) is a set of digital systems that enables countries to safely and efficiently provide economic opportunities and deliver social services." – The Gates Foundation

Similarly, when the United Nations Development Programme (UNDP) partnered with Sri Lanka's Digital Economy Ministry in early 2025 to organise the 'Sri Lanka Digital Public Infrastructure Summit 2025', it highlighted "the critical role of DPI as an enabler in building the country's digital economy with universal DPI safeguards embedded to ensure safety and inclusion."

In this way, common DPI models propagate the need for a foundational layer of digital legal identity, digital payments, and streamlined data transfer. Sri Lanka's National Digital Economy Strategy 2030 outlines a similar digital transformation model for the country. Named the 'Connected Digital Government' model, the government outlines a model that can collaborate, share information, and leverage the government's digital and data infrastructure to serve the public effectively. The targets for 2025 include:

- Implementation of a citizen authentication platform
- Implementation of a government-wide digital payment system
- Implementation of a data-sharing platform for the government
- Increase Sri Lanka's ranking in the Government AI Readiness Index from 105th to 95th

Critics argue that bundling multiple systems under the DPI umbrella disregards important conversations about the unique human rights issues for each component. Civil society has criticised the underlying approach to digital identity systems now deployed under DPI for years, finding them fundamentally incompatible with human rights principles and especially in the context of vulnerable communities. The current push for DPI is seen as rebranding and expansion of digital identity systems already acknowledged as problematic.

With Sri Lanka's long history of corruption and nepotism, there remains a need for independent oversight to block private sector influence over the country's DPI agenda, and the digital ID project in particular, that is not in the public interest.

In this brief, we explore the key DPI developments in Sri Lanka and argue the critical need for closely monitoring them and their effects on the rights of the people.

DPI in Sri Lanka – Key Developments

Sri Lanka's current digital public infrastructure is undergoing a rapid transformation, with several foundational elements in place. Some key developments over the past few years are listed below.

- **Digital identity:** Sri Lanka has initiated the development of a biometric-based Unique Digital Identity Framework (SLUDI). A call for proposals was issued in May 2023 for this framework, which aims to establish a foundational ID platform for issuing new national identity cards to over 16.5 million adult individuals. The platform is intended to enhance digital identity management, improve service delivery, and facilitate e-KYC services for both public and private transactions.

- **Digital payment systems:** The country has seen increasing popularity of digital transactions, with mobile banking applications being offered by banks, telecommunication companies, and third-party providers. Popular services include eZ Cash and mCash, and bill payment applications for utility services. The Central Bank of Sri Lanka (CBSL) leads digitalisation efforts for the national payment system, which includes the Real Time Gross Settlement (RTGS) system for high-value payments and the Common Electronic Fund Transfer Switch (CEFTS) for real-time retail transactions. The LANKAQR code has also been introduced to facilitate direct money transfers from customer accounts to service providers, specifically targeting Small and Medium Enterprises (SMEs).

- **Data exchange and government enterprise architecture:** While government policies such as the Digital Government/Governance Policy, Data Sharing Policy, and the Lanka Interoperability Framework (LIFe) exist, a 'whole-of-government approach' has not yet been fully adopted, leading to state entities often operating within digital silos. To address this, the nationwide Government Enterprise Architecture (GEA) has been developed by the state's Information and Communication Technology Agency (ICTA) to enable seamless and efficient data exchange between various government organisations, facilitated by a National Data Exchange (NDX).

- **Cloud computing infrastructure:** The Lanka Government Cloud (LGC 2.0) serves as the government's cloud computing infrastructure, providing secure and reliable hosting facilities for government applications and systems. While public agencies primarily use LGC 2.0, private companies also utilise international public cloud services. Sri Lanka possesses two tier-3 data centers, operated respectively by telecommunication companies Sri Lanka Telecom (SLT) and Dialog, indicating potential to become an international data hub.

- **Legal and regulatory framework:** Electronic communications and transactions are governed by the Electronic Transactions Act No. 19 of 2006. The Sri Lanka CERT | CC acts as the National Root Certification Authority, and LankaSign is the sole Certification Service Provider.

In 2022, Sri Lanka introduced a comprehensive legislative framework for data protection with the Personal Data Protection Act, No. 9 of 2022 (PDPA), which mandates the establishment of an independent data regulator. Although the PDPA was expected to be operational by March 2025, the government has announced that it plans on amending the act to address certain concerns like AI and investor-friendly regulations. At the same time, concerned civil society and media actors point out that the proposed amendments do not address the initial criticism directed toward the PDPA – such as the "staggering power imbalance between data controllers and citizens".

A Cyber Security Act is also in the pipeline to implement the 2019-2023 National Information and Cybersecurity Strategy, establish the Digital Infrastructure Protection Agency, and empower SLCERT|CC for critical information infrastructure protection.

Despite progress in infrastructure, internet usage in Sri Lanka remains limited due to low awareness and poor digital literacy and skills which means that many existing digital government services are not frequently used by citizens, particularly when offline alternatives are available. The varying levels of digital maturity among governmental entities and potential disruptions caused by changes in political leadership also hinder the adoption of government-wide digital initiatives.

The national digital strategy envisions a "digitally empowered Sri Lanka for innovation, inclusion and sustainable growth" by 2030. To achieve this, the strategy focuses on building a common DPI, encompassing digital ID, payment gateway, and data exchange platform, ensuring scalability and interoperability. It also aims to enhance the use of both public and private cloud services, including implementing a "cloud-first policy" and upgrading the Lanka Government Cloud to a hybrid model with disaster-recovery capabilities.

Although the government has stated that it plans to be human-centric and rights-based in its creation of a digital economy and society, concerns exist over transparency, lack of consultations with diverse stakeholders, and the influence of both private sector and foreign states.

Rights-Based Concerns

The prevailing view often assumes that tools developed in one context can be effectively exported, exemplified by global initiatives like GovStack, which promotes standardised e-government platforms. This risks ignoring specific community needs and sidelining human rights concerns.

By conceptualising DPI as an expansion of existing digital ID systems (often centralised, mandatory, biometric, and lacking safeguards), proponents are entrenching harms already experienced by vulnerable communities. These harms include:

- **Exclusion –** Failures in technology or administration can deny vulnerable individuals access to essential services and benefits
- **Discrimination –** System design choices can amplify existing discrimination or introduce new forms like targeted surveillance or denial of services
- **Cybersecurity risks –** Centralised databases of sensitive personal data are attractive targets for malicious actors, and meaningful remedy is difficult to provide
- **Surveillance –** Centralised data systems with little accountability or statutorily permitted data sharing can lead to abuse, as seen in Venezuela where the national digital ID system is used for surveillance and control
- **Coercion –** When participation becomes de facto mandatory, individuals lose the ability to opt-out, undermining consent and autonomy. Examples include banks in India requiring Aadhaar ID despite court rulings and refugees in Jordan needing iris scans to access aid
- **Private sector involvement –** DPI often involves a significant role for private companies, blurring public-private lines. This can lead to less accountability and transparency, incentivising an "extractive and maximalist relationship" to people and their data
- **Interoperability risks –** While interoperability can support efficient service delivery, it presents significant risks if not properly managed. Without robust data protection, increased data flow among actors amplifies surveillance risks, decreases individual agency over data use, and magnifies the impact of failures across interconnected systems

These rights-based concerns are exemplified in one of the biggest DPI rollouts in recent history – the world's largest digital ID database, known as the 'Aadhaar'. Exploring the complications of India's Aadhaar provides insights into how states and private actors can weaponise DPI to harm citizens in the new age.

The Aadhaar project, despite its stated good intentions, is seen as a cautionary tale where an over-centralised, technologically flawed, and poorly implemented digital identity system has led to widespread exclusion, significant privacy violations, and a potential shift towards a surveillance state, often prioritising commercial and state interests over fundamental human rights.

Practical Difficulties and Exclusion From Services

Aadhaar, contrary to its aim of enhancing inclusion, has become a significant hurdle in accessing welfare benefits and essential services.

Many individuals face problems getting an Aadhaar number due to inadequate biometric quality, the unavailability of "biometric exception" systems, or being too sick or immobile to enroll. Some apply but never hear back or lose their card and cannot get it reissued. Linking Aadhaar is often cumbersome or impossible due to a lack of awareness, physical immobility, or errors in the linking process itself. Inconsistencies in details (e.g. misspelt names) also hinder linking. 'Illegal immigrants' such as Rohingyas or those in Assam have been denied Aadhaar numbers.

Biometric authentication frequently fails, particularly for the elderly, manual labourers, or those with conditions like leprosy, and the Indian government has admitted to high authentication failure rates. Override mechanisms like One-Time Passwords (OTPs) are rarely available on the ground. Updating biometrics, which are not stable over a person's lifespan, is costly and time-consuming. These failures lead to hassles where vulnerable people must be physically carried to authentication points.

These problems lead to severe consequences, including the cancellation or suspension of benefits without notice. Many have had lost access to subsidised rations or have had their pensions delayed or rejected. Basic rights, such as school admission and healthcare, have been denied. There have been documented cases of hunger-related deaths precipitated by mandatory Aadhaar and deaths due to denial of healthcare.

The effort required to avail existing benefits has increased due to longer waits, repeated trips for authentication, or trips to various service centers. Middlemen frequently demand bribes for Aadhaar enrollment, linking, and even benefit disbursement.

Privacy, Surveillance, And Data Protection Concerns

Aadhaar poses a massive threat to the privacy of citizens due to its overreaching influence and data leaks, with the potential to become an oppressive surveillance tool for the state. The Aadhaar Act's design enables surveillance, allowing the sharing of demographic data and authentication records, including for "national security" purposes without clear definitions or checks.

The metadata trails generated by authentication requests provide information about the source of transactions (e.g. banks, hospitals, employers, railway systems), enabling profiling. The aggressive "seeding" of Aadhaar numbers into various government and private databases (often without consent) allows for a "360-degree view" and tracking of individuals across different aspects of their lives, including voter profiling. This consolidation of data can be easily abused by an authoritarian government.

India lacks comprehensive data protection legislation while existing minimal protections do not grant individuals control over their data, allowing the government to compile sensitive personal data without consent. The proposed data protection bill is criticised for giving the state significant latitude and potential exemptions from the law itself. Aadhaar has been accused of failing to take responsibility for data breaches and even filing criminal proceedings against researchers who uncovered security flaws.

The system has been plagued by numerous security lapses. Fraudulent websites phish for information and hundreds of official government websites accidentally made personal Aadhaar data public, sometimes accessible through simple Google searches. Instances include details being sold on WhatsApp for a small fee and personal information being publicly exposed. A high-ranking Aadhaar official's own personal data was hacked and exposed after he challenged hackers. The central database, designed as a single point of failure, is susceptible to breaches, leading to illegal data markets where Aadhaar details are sold. Reproductive health information of women has also been leaked.

The widespread use of Aadhaar numbers has enabled new forms of identity fraud and theft, including fake Aadhaar generation, replication of enrollers' fingerprints, and bank frauds. The printout of the Aadhaar number, often used as a substitute for official photo IDs, lacks traditional security features like microchips or holograms, making it vulnerable to duplication or faking.

Aadhaar's System Design And Misaligned Goals

The project's architecture and implementation have proven counterproductive to its stated benefits, leading to "pain without gain". The system has also been described as "Kafkaesque" due to its disorientingly complex nature. Instead of bringing efficiency, it has increased transaction costs and delayed payments. Rather than enabling transparency, Aadhaar has introduced opacity, making it difficult for individuals to understand or remedy issues when their benefits stop. The Aadhaar Payments Bridge (APB) has led to misdirected payments with no clear redress mechanisms.

The premise that Aadhaar is needed to eliminate fraud from welfare systems is based on a simplification of corruption to "errors of inclusion" (e.g. "ghosts" or "double dipping"). Experts argue that the focus on identity fraud distracts from other, more prevalent forms of corruption and effective reform measures like supply chain improvements or social audits. The supposed "savings" claimed by the government were largely fabricated. The project used the welfare system as a means to quickly scale up its enrollment, regardless of the detrimental impact on beneficiaries.

Tying people to a single, unique digital identity (Aadhaar) can infringe on their right to choose how they identify themselves. The idea of "uniqueness" as a crucial need that only Big ID can fulfill is contested, as it prioritises the state's ability to track individuals over their right to anonymity. Critics argue that the multiplicity of identities is a constitutional right. The process of unique identification is also flawed; the push for enrollment targets led to fake names being entered into the database (e.g., a dog, a spy, or a Hindu god receiving Aadhaar cards).

While projected as a tool for financial inclusion, Aadhaar's model can be data-extractive, benefiting financial institutions by providing "rich digital information" on customers at the cost of the individual's privacy. The primary reason people are unbanked is often a lack of sufficient funds or remote living, not a lack of ID. Linking social protection with financial inclusion can leave vulnerable beneficiaries exposed to risks like predatory loans and debt traps.

The vast biometric database has the potential to revolutionise AI research in India, but it also raises ethical concerns. The Indian government's access to linked data from various services could be used to develop AI programmes that scan activities and patterns to flag individuals as suspicious, potentially turning India into an oppressive surveillance state. Police and criminal tracking systems already aim to integrate with Aadhaar data, with a push for a national DNA database already existing.

Aadhar highlights how DPI can have serious consequences on the rights of citizens. With Sri Lanka taking its first baby steps towards DPI holding hands with partners like India, citizens must remain informed of developments that could potentially impact their lives in permanent ways.

The Need For Monitoring DPI Developments In Sri Lanka

The Ranil Wickremesinghe-administration saw Sri Lanka signing a Memorandum of Understanding (MoU) with the Indian Government to develop the Sri Lanka Unique Digital Identity (SL-UDI) project, facilitated through an Indian grant. The Indian government is expected to float a Request-for-Proposal (RFP) to kick off the project, the Chief Advisor to the President on Digital Economy Dr. Hans Wijesuriya has said in June 2025.

The initial MoU stated that all bidders applying for the tender must be of Indian origin. While an opposition MP in the previous Parliament, current President Anura Kumara Dissanayake raised concerns over the possibility of an Indian entity having access to personal data of Sri Lankan citizens in the digital ID project as the MoU also had a 'maintenance agreement'. Such an agreement would allow the Indian company that develops the platform to ultimately support the system for two further years after it goes live by conducting maintenance.

Dissanayake also alleged in Parliament in August 2023 that the tender to award the contract to build the digital platform had been manipulated to suit a particular bidder. Two Indian companies that bid for the tender were later disqualified.

Since coming into power, Dissanayake's National People's Power-led government has said that they have changed the 'maintenance' clause to ensure that the Indian vendor will hand over all access and control of the platform to a local entity – "most likely a (Sri Lankan) government owned entity, for support and maintenance activities". Once the final set of amendments to the MoU are approved by the Sri Lankan Cabinet, the RFP process is due to be initiated.

According to a January 2025 report in The Sunday Times, the government has indicated that 50% of the total costs of the project will be borne by the Indian government.

This series of events, clouded by a lack of transparency, an administration change, and clauses about private actors having authority over citizens' data highlights the pressing need to closely monitor the developments of the digital ID project, and the overall DPI agenda, in Sri Lanka, lest it becomes another "tragedy of errors" like India's Aadhaar.

Furthermore, the Ministry of Digital Economy is under the direct purview of the country's Executive Presidency. Considering the overarching powers of the Executive President, which have been severely misused to harm citizens in multiple turns of the island's history, this consolidation of digital power at the top raises eyebrows. Despite the government promising an "inclusive digital economy and society", questions remain about consultative processes (or the lack thereof) that go into building this new digital Sri Lanka.

In early 2025, the Ministry of Digital Economy held Sri Lanka's Digital Public Infrastructure summit, in partnership with the UNDP, the Asian Development Bank (ADB), and other collaborators like Citra Lab, the Centre for Digital Public Infrastructure (CDPI), Deloitte, Vital Strategies, the Sri Lanka Association for Software and Services Companies (SLASSCOM), the Federation of Information Technology Industry Sri Lanka (FITIS), the Computer Society of Sri Lanka (CSSL), and Huawei.

Missing from the list of partners are independent organisations that have a history of digital and human rights to ensure necessary guardrails are put in place to stop personal data exploitation or digital colonisation. Although a rights-based approach to DPI is supposed to ensure that accountability and transparency are maintained in processes while the 'extractive' role of private players is reduced, recent events in Sri Lanka regarding DPI are disappointing.

Recommended Next Steps

Sri Lanka's speedy developments in DPI over the last five years, along with the increasing commitment to a digital economy by successive governments, highlight the need to closely monitor policy makers and ensure they take responsible steps forward. Primarily, a need remains to re-evaluate DPI goals to go solely beyond economic advancement and private-sector growth, ensuring they genuinely support community-led innovation and civic life and participation.

To achieve this, the state must foster transparency in all DPI development and implementation processes, especially during changes in political administration, by conducting broad and inclusive consultations with diverse stakeholders, including civil society and affected communities, and implementing independent oversight mechanisms to prevent undue influence from the private sector.

Policy makers must also avoid blindly importing standardised e-government platforms, and instead, tailor DPI solutions to the specific needs and contexts of Sri Lankan communities, ensuring they do not sideline human rights concerns.

Additionally, Sri Lanka must prioritise a human rights-based approach to DPI which:

- Addresses the unique human rights issues associated with each component of DPI, particularly digital identity systems, rather than bundling them without proper consideration.
- Steers clear of highly centralised, mandatory, and biometric-based digital identity systems that lack robust safeguards as these models have historically entrenched harms to vulnerable communities.
- Implements comprehensive data protection legislation that truly grants individuals control over their data, addressing power imbalances between data controllers and citizens.
- Designs DPI systems to prevent their use for unchecked surveillance, profiling, or manipulation and control of citizens.
- Avoids consolidating data in ways that enable a '360-degree view' of individuals and ensures that participation in digital systems is not de facto mandatory, upholding voluntary consent and the ability to opt-out.
- Implements systems that prevent the exclusion of vulnerable individuals from essential services due to technological failures, administrative hurdles, or issues with biometric authentication.
- Implements robust cybersecurity measures for centralized databases as they are attractive targets for malicious actors.
- Enables the public to determine how they are associated with digital identity systems, whether through pseudonyms or to being fully anonymous.

As Sri Lanka embarks on the road of digitalisation, the role of watchdogs, civil society, and journalists is crucial. By becoming knowledgeable in DPI and bridging the information gap that exists in new digital policy initiatives, citizens can strive to ensure that inclusive DPI which safeguards rights is created in the country.

This brief is for informational purposes only. While care has been taken to ensure its accuracy, it has not undergone formal peer review. CommonEdge makes no representations or warranties and accepts no liability for any loss, harm, or offense arising from reliance on or interpretation of its contents.