Zarif Faiaz

Abstract

This paper examines Bangladesh's digital identity ecosystem as an evolving socio-technical infrastructure in which the National Identity (NID) database has become a de facto identity spine across public administration and regulated markets. Using a qualitative, triangulated approach that combines legal and documentary analysis, stakeholder interviews, reconstruction of breach and misuse episodes, and mapping of inter-system access pathways, the study analyses how identity-linked data are collected, linked, and circulated across domains including telecommunications, health, immigration and border control, social protection, and finance.

The analysis finds that the principal risks do not arise from any single database, but from the wider architecture of interoperability and delegated access. Two dynamics are central: (i) the expansion of NID verification through direct institutional connections and commercial gateway models (including the Porichoy API arrangement), which widened downstream access and normalized identity checks; and (ii) the proliferation of informal 'shadow' copies of identity-linked data created for operational convenience, vendor maintenance, and analytics, often outside robust logging, deletion schedules, and audit baselines. These conditions, coupled with vendor backend access, procurement opacity, and a surveillance assemblage in which the National Telecommunication Monitoring Center (NTMC) operates as a central node for communications monitoring and data fusion, enable over-collection, unauthorized sharing, function creep, and, in some cases, insider monetisation of sensitive records.

The paper argues that Bangladesh's existing sectoral laws and administrative practices have enabled data-intensive governance without commensurate rights, safeguards, or enforceable accountability. Drawing comparative lessons from India, the European Union, Pakistan, Singapore, and Australia, it advances a reform pathway centred on a coherent state data governance architecture, genuinely independent oversight (including breach notification and compensation), enforceable vendor controls, proportionality constraints on surveillance, and operationalization of consent and protections for vulnerable groups. The overarching contribution is a grounded map of how 'digital inclusion' infrastructure can become extractive when institutional capacity, legal limits, and technical accountability are misaligned.

1. Introduction

Over the last two decades, Bangladesh has undergone considerable digital transformation in the public sector. At the centre of this transformation sits the national identity (NID) system, established in 2009 under the Voter List Act, 2009 by the Bangladesh Election Commission (EC), initially as a voter-list-with-photographs initiative to strengthen electoral administration, and then subsequently expanded into a general-purpose identity infrastructure under the National Identity Registration Act, 2010. As of early 2025, official figures indicate that the system contains personally identifiable information of over 100 million citizens, underscoring the scale of data consolidated within it and its centrality to electoral administration, service delivery, and identity verification across both public and private sectors.

Within the public sector, the NID system now underpins core e-governance functions, from direct administrative tasks, such as passport issuance, tax filing, land ownership verification and e-mutation, criminal record check, and death and marriage registration, to indirect applications such as the targeting and disbursement of social benefits and state surveillance. Meanwhile, in the private sector, for instance, it enables financial, insurance, e-commerce, cellular, and internet service providers to verify customer identity, support credit assessment, manage fraud prevention, conduct biometric registration, and operationalize a wide array of identity-dependent service provision. Despite growing reliance on centralized identity systems and the close interlinkage of public and private roles within the NID infrastructure, this study finds that the large-scale consolidation of citizen data into interoperable systems has contributed to the emergence of an ecosystem characterized by opacity, legal ambiguity, and structural vulnerabilities.

Bangladesh's approach to digital governance, like most other jurisdictions worldwide, illustrates a paradigmatic case of what legal scholar Julie Cohen has termed the "datafication of governance," where the imperatives of efficiency, administration coordination, and national security frequently override considerations of equity, autonomy, and fundamental rights. While such imperatives are not without justification, numerous media investigations and expert analyses critically emphasize systemic governance failures, limited transparency, maladministration, and weak enforcement allow routine data repurposing, state surveillance, and commercial exploitation by state-aligned entities and private actors without informed public consent or effective oversight. Further compounding these concerns is the recurrent practice of downplaying reported breaches, instead of transparently acknowledging institutional failures, ensuring accountability, or undertaking meaningful remedial and preventive action. For instance, the 2023 data leak reportedly involving over 50 million citizens' records—exposed via the website of the Office of the Registrar General, Birth & Death Registration—underscores how deeply flawed the current system is in its treatment of personal data. In the immediate aftermath of the incident, senior government officials downplayed institutional responsibility, asserting that no problems had occurred at the data centre while attributing the breach to isolated website vulnerabilities, without addressing broader questions of accountability or assuring meaningful systemic remedial and preventive measures to avert recurrence.

This report aims to map the architecture of Bangladesh's digital identity and data governance systems, interrogate their access control mechanisms, and evaluate how data is shared, commodified, or repurposed by various actors. Using a multi-method approach, it combines stakeholder interviews, legal analysis, technical documentation, and case study investigations to examine the institutional infrastructures and private-sector interests that undergird digitalization and digital public administration in Bangladesh.

Conceptually, the study situates Bangladesh's identity infrastructure within wider debates on the datafication of governance, surveillance assemblages, and data extractivism in the Global South. Digital identity systems are treated here as socio-technical assemblages that produce infrastructural power: they enable the state and its intermediaries to classify, verify, and govern populations, while simultaneously creating incentives and opportunities for commercial appropriation of personal data when vendor relationships, procurement practices, and enforcement institutions are weak.

The report pursues four interlinked objectives: first, to map the architecture of Bangladesh's identity and data ecosystem and identify the main access pathways through which NID-linked information circulates across sectors; second, to analyse the legal, institutional, and technical controls (and gaps) that shape data sharing, retention, and repurposing; third, to scrutinise the role of private vendors and intermediaries as de facto data controllers through backend access, vendor lock-in dynamics, and opaque contractual arrangements; and fourth, to assess the rights and distributive impacts of data exploitation, particularly for poor and marginalized groups whose ability to refuse data collection or contest misuse is limited.

The inquiry is guided by four questions: who exercises practical authority over identity-linked data in Bangladesh; how access and interoperability are operationalized across state and market actors; how consent, notice, and purpose limitation function (or fail) in everyday service delivery; and what reforms are necessary to build enforceable accountability while preserving legitimate administrative functions.

The remainder of the paper is structured as follows. Section 2 sets out the theoretical and analytical framework. Section 3 details the methodology. Sections 4 through 6 present the empirical analysis, covering the architecture and cross-linkages of sectoral systems, the role of private vendors, and the mechanisms through which data exploitation and surveillance produce disproportionate harms. Section 7 develops a comparative perspective drawing on selected international models. Section 8 proposes a reform agenda across legal, institutional, and technical domains. Section 9 concludes with implications for digital sovereignty, democratic accountability, and data justice in Bangladesh.

2. Theoretical and analytical framework

Understanding the governance failures and data exploitation risks within Bangladesh's digital identity systems requires an interdisciplinary analytical lens. This study draws on critical data studies, surveillance scholarship, and theories of digital colonialism to examine the structural dynamics at play. The framework integrates concepts from data justice and legal-institutional analysis to interrogate how state and private actors collect, process, and control citizen data with limited transparency or accountability.

2.1 Critical data governance and infrastructural power

Digital identity systems like Bangladesh's NID architecture are not merely technical solutions; they are socio-technical assemblages that embody specific power relations. As Ruha Benjamin notes, data systems are often shaped by "discriminatory design" and institutional logics that reproduce social hierarchies. In this context, the state's use of centralized identity and biometric databases, coupled with surveillance infrastructure, must be understood as a form of infrastructural power, where control over data becomes a mechanism for governing populations. The theoretical lens of data governance thus becomes crucial: it emphasizes not only who owns data, but also who can access, share, and decide its purpose. In Bangladesh, governance failures manifest in weak access control, porous legal frameworks, and the unaccountable role of vendors. These failures are not incidental; instead, they are products of institutional neglect and deliberate policy vacuums that enable unchecked data extraction under the guise of efficiency and national security.

2.2 Surveillance and securitization of identity

Bangladesh's digital infrastructure increasingly resembles what David Lyon terms a "surveillance assemblage": heterogeneous datasets, including identity records, telecoms metadata, health information, travel and financial traces, are integrated to generate actionable intelligence about individuals and groups. The National Telecommunication Monitoring Center (NTMC) exemplifies this shift from siloed databases to networked systems: through operator-facing interfaces and inter-agency feeds, NTMC functions as a central node for communications monitoring and associated identity checks, illustrating how surveillance today is produced by data linkages rather than any single repository.

The legal basis invoked for this model lies in sections 97 and 97A–C of the Bangladesh Telecommunication Regulation Act, 2001, which empower the Ministry of Home Affairs to order interception and require operator cooperation, providing a legal hook for establishing a central lawful-interception facility. However, whether the operation of such a facility meets constitutional and international human rights standards turns on the presence of published, binding implementing rules that specify prior authorization (by whom and on what grounds), targeting criteria, time limits and retention, auditability, and avenues for redress. As long as such rules are unpublished, incomplete, or non-existent, the regime risks failing the tests of legality, necessity, and proportionality that flow from constitutional privacy guarantees and comparative human-rights doctrine.

The assemblage is typically justified in the language of national interest, security, and crime prevention, aligning with scholarship on the securitization of identity. In these conditions, personal data are not neutral administrative artefacts; they become instruments of classification and control. Crucially, much of this processing occurs without meaningful citizen notice or consent, producing an asymmetry of visibility in which state actors enjoy expansive insight while individuals lack transparency and effective recourse.

> **Bangladesh's digital identity systems function as political infrastructures where weak governance, securitization, and opaque public–private control enable systematic data exploitation. Framed by security and efficiency narratives, these systems reproduce colonial and authoritarian power asymmetries, undermining transparency, consent, and data justice.**

2.3 Digital colonialism and data extractivism

The privatization of critical digital infrastructures and the outsourcing of sensitive systems to domestic and international vendors point to a deeper structural condition: digital colonialism. Defined by scholars like Nick Couldry and Ulises Mejias, digital colonialism refers to the large-scale appropriation of citizens' data resources by a few dominant state and non-state actors, without proportionate compensation or the informed consent of the subjects from whom data is extracted, thereby reproducing and extending historical colonial power relations under contemporary capitalism.

In Bangladesh, several media reports reveal that companies like Tiger IT Bangladesh Limited have not only built core identity and surveillance platforms but have also retained privileged backend access to citizen data, often without enforceable limitations or transparent contracts. This creates a system where data is commodified and monetized through opaque deals, with little benefit or awareness on the part of data subjects. Moreover, these vendors often maintain ties to political or security elites, blurring the lines between public interest and private profit.

This framework positions digital identity not as a neutral innovation but as part of a global extractivist order where data replaces natural resources as the site of exploitation. Without strong legal and institutional constraints, such extractivism risks becoming entrenched, exacerbating existing inequalities while cloaking itself in the language of development.

2.4 Institutional and governance dynamics

Bangladesh's state authority and bureaucratic governance exhibit complex legacies shaped by colonial history, political struggles, and entrenched institutional practices. The bureaucratic system reflects a hybrid model influenced by Weberian legal-rational principles intertwined with traditional patronage and politicization dynamics unique to the Bangladeshi context. This hybrid bureaucratic governance limits transparency and accountability, often privileging elite interests and state control over citizen-centric governance.

The colonial legacy of centralized administration created structures geared more towards control and extraction than participatory governance, which has persisted post-independence. Despite efforts at democratization and digital modernization, the state retains authoritarian features, often framed as competitive authoritarianism, where electoral processes coexist with restricted opposition, institutional control, and limited civil society autonomy.

The institutional dynamics are further shaped by the historical trajectory of political consolidation under dominant parties, where bureaucratic politicization hampers reforms and allows state agencies disproportionate discretion and secrecy, especially in sensitive domains such as digital identity and data governance. Structures of authority in Bangladesh tend to prioritize regime stability and political control over rights-based data governance, reflecting the continued power asymmetries rooted in historical and political processes.

In the context of digital governance and data exploitation, this theoretical lens elucidates why institutional inertia, weak enforcement, and blurred boundaries between state and private vendors prevail, facilitating routine non-transparent data access and repurposing without public accountability.

2.5 Toward a data justice lens

Finally, the analytical framework foregrounds the principle of data justice. As articulated by Linnet Taylor and others, data justice calls for systems that respect agency, equity, and rights—not just efficiency. It demands transparency about how data are used, accountability for misuse, and the institutional capacity to provide redress. In contexts like Bangladesh, where legal remedies are absent and political pressures are high, embedding data justice requires structural reforms that redistribute both power and knowledge in the digital domain. By employing this multi-layered framework, the report seeks to move beyond surface-level critiques of privacy to interrogate the deeper political economy of data governance in Bangladesh. It treats digital identity systems not merely as policy tools but as contested infrastructures whose design and operation shape the rights, dignity, and futures of citizens.

3. Methodology

This research adopts a multi-pronged qualitative methodology to examine how data access, control, and misuse operate within Bangladesh's digital identity ecosystem. Given the opacity of government systems and the absence of transparent public documentation, the study emphasizes triangulation across sources—official documents, stakeholder accounts, technical systems analysis, and media reports—to reconstruct an accurate picture of governance practices. The methodology is shaped by a commitment to transparency, equity, and systemic inquiry, aligning with critical data studies and rights-based research traditions.

3.1 Research design and objectives

The study is grounded in a diagnostic research design aimed at identifying governance failures, institutional power asymmetries, and reform opportunities within Bangladesh's digital identity and data infrastructure. The central research questions guiding the methodology are:

- How is citizen data collected, stored, and accessed across key government databases in Bangladesh?
- What legal, institutional, and technical controls govern these access pathways?
- What roles do private vendors, contractors, and intermediaries play in handling and potentially misusing sensitive data?
- What accountability mechanisms exist to address misuse, mission creep, or breaches?
- How can governance models be improved to ensure transparency, citizen control, and data protection?

These questions are explored across three empirical domains: (1) intra-governmental access and surveillance, (2) public-private partnerships and vendor roles, and (3) comparative models and reform pathways.

> **This study employs a triangulated qualitative methodology combining legal analysis, stakeholder interviews, breach case studies, and data-flow mapping to examine governance failures in Bangladesh's digital identity ecosystem. By integrating comparative and rights-based frameworks, it reconstructs opaque data practices while accounting for institutional secrecy, political sensitivity, and structural limitations.**

3.2 Data collection strategies

3.2.1 Document and legal analysis

A detailed review was conducted of over 30 policy and legal instruments, as well as publicly available memorandum of understandings, request for proposals, contracts, and procurement documents involving vendors were analyzed to understand access, control, and contractual obligations concerning citizen data.

3.2.2 Stakeholder interviews and testimonies

Interviews and off-the-record discussions were conducted with a cross-section of stakeholders within Bangladesh, including:

- Government officials from the Election Commission, the Ministry of Posts, Telecommunications and Information Technology, and law enforcement and intelligence agencies
- Representatives from civil society, legal advocacy groups, and digital rights organizations
- Journalists who have investigated data leaks and procurement irregularities
- Information technology sector professionals and former contractors involved in digital governance projects
- Legal experts, including lawyers and legal academics

These interviews provided insight into the informal practices, political economy, and institutional workarounds that shape actual data access and misuse, often in contrast to formal rules.

3.2.3 Breach and misuse case studies

The research includes granular case studies of several major data misuse events, including the 2023 birth registration data leak reportedly affecting over 50 million records, the 2023 surveillance breach at the NTMC, vendor-related controversies, and unauthorized data sharing by public institutions. These case studies were reconstructed using investigative reports, interviews, and leaked technical documents, with a focus on tracing the data flow, identifying governance and accountability failures, and evaluating the adequacy of institutional responses to large-scale data misuse.

3.2.4 Mapping data flows and access pathways

To visualize systemic vulnerabilities, the study constructed data flow maps based on technical specifications, and service integration models (e.g., Porichoy API, SIM registration interfaces). These maps document where personal data is collected, who accesses it, how it is stored, and the legal or informal mechanisms that enable these flows. Specific attention was given to systems integrating NID data with health records, telecom metadata, immigration logs, and financial identifiers. For clarity of scope, this report focuses on the NID as public infrastructure and its sanctioned interfaces with external entities; it does not purport to inventory the broader universe of private data infrastructures and commercial data flows that may operate beyond these formal linkages.

3.3 Comparative and normative lens

To contextualize the findings from Bangladesh within broader global debates on digital governance, this research integrates comparative insights from a diverse set of national models. These include both rights-protective regimes (such as the European Union, Singapore, and Australia) and surveillance-heavy infrastructures (such as China), including a comparison with neighbours such as India (Aadhar). The aim is not to transplant foreign models wholesale, but to extract actionable principles, particularly around consent, access control, institutional oversight, and vendor accountability.

Rights-protective frameworks

European Union: The EU's General Data Protection Regulation remains the global benchmark for legally enforceable privacy rights. Key lessons include the operationalization of data minimization, informed and revocable consent, breach notification, and user access rights. GDPR's institutional backbone, independent data protection authorities, illustrates the importance of enforcement, not just principle-setting.

- **Singapore:** Singapore's National Digital Identity demonstrates a functional model of user-centered consent, API-based secure access, and strict vendor governance. Myinfo allows granular, transaction-specific data sharing with user approval. Vendors are tightly regulated, with audits and cybersecurity compliance required. Singapore's handling of the TraceTogether privacy backlash also shows the value of public trust and legislative responsiveness. For Bangladesh, Singapore offers a pragmatic context in which digital transformation has been aligned with inclusion and transparency.
- **Australia :** Australia's Protective Security Policy Framework includes mandatory data handling standards for vendors, enforceable contracts, and routine audits. These frameworks reduce backend access abuse, a persistent issue in Bangladesh. PSPF emphasizes that cybersecurity and privacy cannot be outsourced, and public agencies must remain accountable for vendor conduct.

Surveillance-oriented models

- **China:** China's digital identity and surveillance infrastructure offers a stark contrast. With pervasive real-name registration laws, interlinked databases, and broad exemptions for state agencies, China illustrates how digital identity systems can evolve into tools for centralized control and political repression. Although it has a personal information protection law, its utility is limited by the dominance of national security justifications. Bangladesh must be wary of adopting technical systems or data centralization logics without concurrent legal checks.

These comparisons deepen the normative lens of this study by emphasizing that technological capacity does not guarantee good governance. Where institutional autonomy is weak, procurement is opaque, and surveillance powers are unchecked, digital identity systems can exacerbate exclusion, discrimination, and abuse. Conversely, strong consent frameworks, secure architecture, and inclusive design—as seen in Singapore—can foster trust, accountability, and citizen empowerment.

3.4 Ethical considerations

Given the sensitivity of the data and the political context, strict precautions were taken to anonymize all stakeholder testimonies and redact sensitive identifiers in case study descriptions. All data collection was guided by the principles of informed consent, confidentiality, and harm minimization. No system was tested or probed in ways that could compromise its security; analysis focused on publicly reported breaches and public domain data only.

3.5 Limitations

This study is constrained, at the research design stage, by the scale and fluidity of Bangladesh's identity ecosystem. The analysis foregrounds the NID as public infrastructure and maps its sanctioned or widely reported interfaces with other sectors; it does not claim to inventory the full universe of private data infrastructures, data brokerage practices, or informal commercial datasets that may operate beyond, or parallel to, state-linked systems. This scoping choice was necessary for analytic tractability, but it means that the paper captures only a portion of the wider political economy of data extraction in Bangladesh.

At the documentary evidence stage, limited transparency around government systems and procurement restricted the ability to verify institutional arrangements through primary documentation alone. Many memoranda of understanding, integration specifications, security policies, and vendor contracts are not publicly available, while those that are accessible are often partial, redacted, or mediated through secondary reporting. This evidentiary constraint is particularly salient for security-linked infrastructures and for vendor arrangements where contractual provisions on access control, retention, and auditability are decisive but difficult to examine directly.

At the stakeholder engagement stage, interview-based evidence was shaped by access barriers and the political sensitivity of the topic. Some relevant actors declined to participate, and all participants requested strict anonymization, which limited the extent to which institutional roles and claims could be attributed or cross-examined in detail. Fear of reprisal and professional risk may have produced conservative accounts (under-reporting of misconduct) in some instances, while in others it may have encouraged strong allegations that could not be independently corroborated. The study mitigates these risks through triangulation, but they remain inherent constraints.

At the comparative analysis stage, the use of international models (including India, the European Union, Singapore, and Australia) is necessarily selective and interpretive. Comparative frameworks can illuminate design and governance options, but they do not transfer mechanically across contexts with different constitutional traditions, enforcement capacity, procurement regimes, and political constraints. The comparisons therefore function as normative reference points rather than prescriptive templates.

Finally, at the synthesis and recommendations stage, the study advances reform pathways without undertaking detailed costing, implementation sequencing, or organizational change modelling. Institutional reform in Bangladesh will depend on budgetary allocations, bureaucratic incentives, and political will that cannot be fully assessed through desk-based research. Moreover, the regulatory landscape is dynamic, and both legal instruments and technical systems continue to evolve; some factual claims may shift as contracts, platforms, and mandates change in coming years. The recommendations should thus be understood as a rights-based direction of travel, to be operationalized through further technical assessment and participatory policy design.

4. Mapping Bangladesh's digital identity and data systems

Bangladesh's digital identity and data ecosystems are shaped by an expansive, interconnected set of databases, regulatory frameworks, and institutional actors. These systems, though established to modernize service delivery and governance, operate through a fragmented and largely opaque architecture. This section provides a detailed map of the key data systems—including their scope, integration points, responsible entities, and vulnerabilities—centered on the NID database and extending across multiple interconnected domains of public and private administration.

4.1 The national identity system as foundational infrastructure

At the core of Bangladesh's digital public infrastructure for personal data management stands the national identity (NID) system, administered by the Bangladesh Election Commission (EC). Originally developed for voter registration under the Voter List Act, 2009, the NID has since been repurposed as a de facto citizen national identification and verification backbone for the state, while also serving as the primary interface through which private actors authenticate individuals against public records. The database stores extensive biometric and demographic attributes—names, addresses, parentage, genders, dates of birth, fingerprint and palm templates, signatures, and facial photographs—and now covers over 100 million citizens, seemingly making it the country's largest repository of core personally identifiable data.

Within the public sector, NID underpins direct administrative functions, such as passport issuance, tax filing, land ownership verification and e-mutation, criminal record tracking, and death and marriage registration, as well as indirect functions such as eligibility assessment and disbursement of social benefits. In parallel, through state-run verification gateways (e.g., e-KYC and identity APIs), the NID infrastructure enables a wide range of private-sector operations, including customer verification, credit assessment, fraud prevention, and service activation across banking, telecommunications, mobile financial services, utilities, and other identity-dependent sectors. This is enabled by sections 14(3) and 16 of the now reportedly repealed National Identity Registration Act, 2023 and sections 13(3) and 13A of the National Identity Registration Act, 2010, which explicitly allows institutions and individuals to request access to the identity database, and confers legal mandate for EC to share citizens' personally identifiable information.

Central to understanding the operation of the NID system beyond its role in electoral administration are the governance models through which identity verification and data access are operationalized. Bangladesh's identity infrastructure is stitched together through a set of technical conduits that all, in one way or another, resolve back to the EC's NID system. However, in practice, there are two distinct, but frequently conflated, access pathways.

First, the EC offers direct access to certain public bodies and through private institutions via government-to-government and government-to-business channels, under agreements executed directly with these entities. As of December 2024, at least 183 such organizations reportedly had active identity verification arrangements with EC, without any intermediary.

Second, a commercial application programming interface (API) gateway model branded Porichoy, developed by the Bangladesh Computer Council (BCC) and operated by Digicon Global Services Limited., opened identity-verification services to a much broader market. BCC itself received access to the database under an agreement executed with the EC. By October 2024, more than 450 companies used Porichoy's services, generating roughly eighty million verification calls and about BDT 1.12 billion in revenue, of which 60-90% was reportedly retained by Digicon Global Services Limited and remaining to be disbursed to EC and BCC. Both regulatory agencies and private entities were compelled to use Porichoy. However, this arrangement allegedly violated third-party data commercialization restrictions in the cabinet-approved agreement, and was revoked in December 2024.

Across multiple sectors, one of these two NID system accessways functioned as an identity verification pipeline, which, in turn, enabled secondary verification across services. For instance, in mobile telecommunications, regulator-mandated SIM registration links each applicant's NID with biometric information captured at retail points, with operators verifying identities through EC-backed services and retaining KYC records in accordance with regulatory requirements; the resulting MSISDN–NID linkage may then be reused by mobile financial service providers, such as bKash, Nagad, and Rocket, to perform e-KYC by relying on the pre-existing verified association without re-collecting identity information. Similarly, in education and social protection, school and stipend management information systems associate beneficiaries with NID and verified mobile numbers, enabling government-to-person disbursements through banking and mobile financial channels. Meanwhile, in the health sector, programmes such as the Surokkha vaccination platform, operated by the Directorate General of Health Services (DGHS), link eligibility and certification to NID, with mobile numbers used for service notifications. Border management systems likewise associate e-passport biometrics with NID to support watch-list checks at e-gates, typically through vendor-operated biometric components. Collectively, these arrangements create interconnected data flows across public service systems, often supported by private contractors — including Digicon Global Services Limited, Synesis IT PLC, Computer Network Systems Limited, and Tiger IT Bangladesh Limited — responsible for developing, hosting, or maintaining the underlying technical components.

Taken together, this ecosystem appears to enable systemic overreach, not through any single technical feature, but through the expansion of identity verification across hundreds of downstream agencies and service providers via gateways shaped by commercial incentives and limited transparency, without commensurate controls by the EC over purpose limitation, data minimization, logging, vendor privileges, or meaningful citizen consent. Combined with the scale and linkability of the system — where services are keyed to NID, often bound to verified mobile numbers and, in some cases, biometrics — this architecture has produced a surveillance substrate with limited avenues for accountability or user redress.

> **Bangladesh's NID system functions as a central identity spine linking health, telecom, finance, welfare, and security databases, creating deeply interconnected data flows with minimal transparency or control. Fragmented governance, informal replication, vendor-mediated access, and weak sectoral laws have produced systemic vulnerabilities, enabling surveillance overreach, data leakage, and unaccountable data exploitation across the state.**

4.2 Sectoral data (non-exhaustive, indicative) ecosystems and cross-linkages

Health Sector

During the COVID-19 pandemic, in January 2021, the DGHS and the Department of Information and Communication Technology launched the Surokkha platform to register, schedule, and track vaccinations. Surokkha recorded registrations and dose administrations for over 86 million NID cardholders, alongside additional ~2 million vaccinations processed using passports and ~20 million using birth certificates, collectively capturing non-static health, communication, and identity information for over 60% of the country's population. However, there have been no comprehensive or explicit policies governing data retention, secondary use, or privacy for NID-linked data processed through Surokkha. A subsequent report indicates that DGHS shared citizens' sensitive information with third parties, although both the identity of these recipients and how the data have been handled, accessed, retained, or commercialized within or beyond the health system remains unclear.

Telecommunication Sector

Since the mid 2010s, the Bangladesh Telecommunication Regulatory Commission (BTRC) has mandated, under the Bangladesh Telecommunication Regulation Act, 2001 and secondary legislations, biometric SIM registration using NID and fingerprint verification. Operators must connect with the EC's NID system to validate customer identities and are required to retain metadata, including call records, SMS logs, device identifiers, and location data, for up to twelve years. With approximately 187 million registered cellular subscriptions—of which around 115 million are active mobile internet users—mobile SIM registration constitutes one of the largest single sources of personal data collection in Bangladesh, and the continued use of cellular and internet services on mobile device generates continuous, non-static streams of real-time information, including call detail records, location data, internet usage metadata, device identifiers (such as IMEI), messaging logs, and network interaction data.Both the legislations and regulatory frameworks consolidate and centralize data collection and surveillance authority within the NTMC, under the Ministry of Home Affairs, which plugs into telecommunication operators' networks and aggregates citizens' personal data into a surveillance dashboard. In 2023, NTMC's database was compromised, exposing sensitive information such as NID information, call logs, metadata, bank balances, address, biometrics, and passport details, amongst other information — demonstrating how technical integration without effective oversight, adequate governance protocols, or robust privacy measures can lead to data leaks. Additionally, NTMC operates an intelligence sharing platform for verification and investigation purposes, accessible by approximately 500 officials from 42 organizations; and, since early 2024, at least two external senior law enforcement agents are reportedly under investigation for excessive access to the platform and unauthorized data transfer to third parties. Operating in the opposite direction, reports by Tech Global Institute and the Office of the United Nations High Commissioner for Human Rights indicate that the NTMC has been actively surveilling citizens, presumably using a combination of information collected from operators and imported spyware, in purported violation of human rights.

Immigration and Border Control

Different state agencies handle immigration and border control data. For instance, the Department of Immigration and Passports, under the Ministry of Home Affairs, maintains a biometric passport database that integrates passport issuance and related operations with the NID system for identity validation. Meanwhile, the Civil Aviation Authority of Bangladesh, under the Ministry of Civil Aviation & Tourism, collects data related to aviation and passenger movements, while the Special Branch, the internal security intelligence wing of the Bangladesh Police operating under the Ministry of Home Affairs, is responsible for immigration control. Each of these agencies accesses EC's NID infrastructure under a direct contractual arrangement, with different stacks of the underlying technology built, operated, or maintained by private contractors. It remains unclear whether, and to what extent, these public and private actors commercialize immigration and border control data, or otherwise formally or informally share such data with third parties, and under what legal or regulatory frameworks.

Social Welfare

Numerous social protection initiatives, including cash transfers, pension disbursements, and education stipends, use the NID database for beneficiary verification, with two core state platforms mediating these flows. First, iBAS++, the government's public-finance software developed by Oracle and managed by Ministry of Finance for budgeting, payroll, pensions, and beneficiary payments, incorporates NID fields for enrolment and authorization.; Second, EkPay, a government payment gateway under the a2i programme that aggregates public-to-government payments and interoperates with banks and mobile financial services, is also linked to the EC's NID infrastructure. In fact, welfare-related data flows are often multi-directional: telecommunication data (for mobile banking), education records (for school stipends), and land databases (for rural subsidies) link back to NID entries, producing expansive, cross-sector personal profiles. At present, there is no centralized consent or accountability mechanism governing these composite linkages, which amplifies the governance risks. It also remains unclear whether, and to what extent, these public and private actors commercialize welfare-related data, or otherwise formally or informally share such data with third parties, and under what legal or regulatory frameworks.

A non-exhaustive list of personal information and data categories collected by various government agencies in Bangladesh

The table below provides a preliminary, indicative mapping of selected Bangladeshi public authorities that collect and process citizens' personal data in the course of identity management, service delivery, regulatory oversight, and security functions.

Agency names use formal titles and reflect their parent ministries or their divisions where relevant—for example, the Department of Immigration and Passports under the Ministry of Home Affairs; the Directorate General of Health Services under the Ministry of Health and Family Welfare; the Directorate of Primary Education under the Ministry of Primary and Mass Education; the Office of the Registrar General, Birth & Death Registration under the Local Government Division, Ministry of Local Government, Rural Development and Co-operatives; the Bangladesh Telecommunication Regulatory Commission under the Posts and Telecommunications Division, Ministry of Posts, Telecommunications and Information Technology; and the National Board of Revenue under the Internal Resources Division, Ministry of Finance.

The data categories, example data fields, and collection and storage methods listed are illustrative rather than exhaustive and should not be read as a definitive inventory of all attributes held by any institution, nor as a complete description of system architectures or retention practices. In practice, the exact fields collected, the biometric modalities used, and the storage and processing arrangements may vary by programme, implementing partner, and time period (including differences between statutory mandates and operational practice). The mapping is compiled from desk-based review of publicly available institutional materials (such as agency portals and programme systems), relevant legal and policy documentation, and the broader research design and documentary review underpinning this study.

Finally, the institutions listed are not the only public entities involved in collecting, sharing, or linking citizen data. A wider ecosystem of public bodies, state-owned entities, and contracted service providers may access or interoperate with identity and verification infrastructures (including connectivity to EC's NID-related databases) through formal integrations, delegated functions, or routine verification practices.

Agency	Illustrative Data Categories	Illustrative Personal Information Details	Illustrative Collection Methods
Bangladesh Election Commission (under Prime Minister's Office)	Personal identity data, Biometric data, Voter registration	Name, photograph, address, date of birth, parents' names, signature, fingerprints, iris scans, facial images, retinal scans, contact details, electoral roll details	Direct biometric registration at local offices, fingerprint scanners, cameras; document verification
Bangladesh Financial Intelligence Unit (BFIU, under Ministry of Finance)	KYC data, Financial risk data, Compliance information	Name, parents' names, spouse's name, date of birth, gender, profession, mobile number, addresses, biometric fingerprint (≥80% match), face recognition, financial risk grading, transaction patterns, beneficial ownership, UNSCR/PEP/adverse media screening	Electronic customer onboarding at banks; real-time NID connectivity; biometric capture devices
Department of Immigration and Passports (under Ministry of Home Affairs)	Passport information, Border control data, Document authentication	Personal details (as above), travel history, visa records, immigration status, passport verification, lost passport records	Online application systems, physical document submission, biometric capture devices
Bangladesh Police (under Ministry of Home Affairs)	Crime statistics, Police clearance data, Investigation records	Personal identification for police clearance, detailed crime data (murder, robbery, theft, cybercrime), witness statements, evidence files	Online clearance applications, crime reporting systems, digital forensic analysis
Directorate General of Health Services (under Ministry of Health and Family Welfare)	Patient health records, Disease surveillance, Health facility data	Medical histories, treatments, health outcomes, demographic details, epidemic and pandemic data, medical staff information, facility resources	District Health Information System (DHIS2), web-based health data entry, digital patient records
Ministry of Education	Student enrollment data, Teacher information, School infrastructure	Student names, age, grade-wise enrollment, attendance, repeater info, teacher qualifications, training records, employment details, school facilities (ICT, classrooms, buildings)	IPEMIS digital enrollment system; annual census via digital questionnaires; data entry by head teachers
Bangladesh Bank (under Ministry of Finance)	Banking statistics, Financial sector data, Customer complaint data	Account details, deposit and loan data, interest rates, money supply data, exchange rates, customer grievance data, complaint resolution history	Electronic data reporting from banks quarterly; digital customer complaint forms, hotlines
Ministry of Land	Land records, Survey data, Registration records	Record of rights, khatian documents, land ownership info, mutation certificates, land transfer deeds, mauza maps, plot boundaries	Digital GPS-based land surveys; revisional survey of land holdings (~40 million); online verification systems
Bangladesh Telecommunication Regulatory Commission (BTRC, under Ministry of Posts, Telecommunications and Information Technology)	Subscriber information, Device registration, Network monitoring	SIM subscriber details (name, address, biometric data), IMEI device registration (handset identification), network service quality and compliance	Biometric SIM registration; IMEI registration database (NEIR); automated network monitoring systems
National Board of Revenue (under Ministry of Finance)	Taxpayer information, Trade data, Compliance records	Tax identification numbers (TIN), income declarations, import and export details, customs declarations, tax payment history, audit records	Electronic tax filing systems; online customs clearance via HS codes; digital trade declarations
Office of the Registrar General, Birth & Death Registration (under Ministry of Local Government, Rural Development and Co-operatives)	Birth registration, Vital statistics, Identity verification	17-digit birth registration numbers, name, date of birth/death, parental details, population demographics, birth and death rates	Online registration via BDRIS; hospital-based registration; local registrar offices

As this section demonstrates, sectoral institutions, policy frameworks, and technical systems in Bangladesh increasingly anchor the country's digital governance architecture in the NID infrastructure as a common identity spine. Across the public sector, and much of the private sector, domains including health, telecommunications, immigration, welfare, finance, and border control no longer operate as isolated databases but as interconnected components that rely on NID-based verification to enable access, eligibility determination, monitoring, and enforcement. This deep interconnection means that compromise, misuse, or weak governance at any single node, whether arising from misconfiguration, unauthorized access, vendor practices, or downstream data replication, can have cascading effects across multiple sectors, allowing, for instance, partial records to be recombined into comprehensive individual profiles. As identity-linked data circulate across public agencies and private intermediaries without consistent safeguards, the resulting risks extend beyond isolated breaches to systemic vulnerabilities, undermining data protection, accountability, and trust in the integrity of the national identity system as a whole.

4.3 Informal and/or unregulated data ecosystem

One of the most significant findings of this research is the prevalence of shadow copies of citizens' personal data, that is, full or partial replicas of identity-linked datasets created outside formal architectures. These arise from everyday "operational fixes" (such as offline fallbacks, latency reduction, batch de-duplication, test/staging environments, or ad hoc analytics) and are often held by line units or vendors with weak change control, minimal logging, and unclear deletion schedules. Because such replicas often sit beyond formal data-sharing agreements and security baselines, they accumulate stale credentials, default configurations, and unpatched services, thereby expanding the attack surface while undermining accountability.

A now-canonical example is the Office of the Registrar General, Birth & Death Registration (ORGBDR). Several investigations reported that ORGBDR accessed the NID database to support identity checks within the birth and death registration workflow and seemingly hosted those data on an unsecured server, precipitating the 2023 exposure of more than 50 million records—including names, phone numbers, and other identifiers. The incident illustrates a recurrent pattern: parallel datasets created for operational convenience, then left misconfigured or insufficiently governed, even where contractual guardrails formally exist. However, once such datasets are untethered by contractual controls, as can occur through unauthorized third-party sharing, they become widely accessible through informal, unregulated, or publicly exposed channels beyond the originating system and susceptible to unauthorized redistribution and commercialization.

Authorized secondary NID access points, ranging from ministries and regulatory bodies to private actors like banks, mobile financial service providers, telecommunication service providers, payment gateways, social-protection platforms, often depend on chains of vendors and field agents. Along these chains, client information, API keys, VPN accounts, and admin logins are informally shared to meet contractual obligations, after-hours support, or retail pressures. This practice spawns unregistered, off-ledger access nodes that can pull NID-linked data while appearing in logs only as the primary institution. These shadow pathways defeat purpose limitation and data minimization, erase actor-level accountability (as forensics cannot conclusively answer who accessed what, when, and why), and erode integrity and confidentiality as long-lived keys leak into staging and analytics environments beyond audit reach. For example, banks or telecommunication service providers may share eKYC data, specifically phone numbers to third party vendors for call centre purposes, who may then share it to other vendors for marketing purposes, all without customer consent or knowledge.

According to those interviewed for this study, a permissive informal market exists in which citizens' personal information can be obtained for a price through multiple pathways: unregulated secondary circulation, where detailed datasets, including NID-linked information, are available for sale by private actors; intermediated access, in which additional details are aggregated from disparate public-sector databases; and, in some instances, facilitation by personnel within public bodies in exchange for nominal inducements. One respondent observed that this informal marketplace has facilitated electoral manipulation in past elections, including the alleged use of NID records associated with deceased citizens, overseas migrant workers, and, in some cases, living individuals without their knowledge or consent, to cast votes on their behalf. Another respondent reported that the same unregulated market enables the creation of false identities, including through the manipulation or substitution of photographs on printed NID cards, which are then used for purposes such as property transfers, accessing social benefits, or opening bank accounts for illicit activities. It was further noted that these services are reportedly offered through informal commercial networks operating openly in areas such as New Market, Mohammadpur, and Uttara, indicating the presence of a localized, thriving trade in identity-related services beyond formal regulatory oversight. While accounts varied in scope and specificity, the convergence of these perspectives points to a systemic governance failure in which weak controls, fragmented oversight, and blurred public-private boundaries have normalized unauthorized access to sensitive personal data, notwithstanding the formal legal protections intended to prohibit such practices.

Another example of how this fragmentation scales is the telecommunication sector. Bangladesh's telecoms field is a fragmented, security-led space where overlapping authorities—BTRC and the Posts & Telecommunications Division on the regulatory side, and NTMC, Bangladesh Police, and other law enforcement and intelligence agencies under the Ministry of Home Affairs on security and surveillance—interact with private operators under broad monitoring and interception powers. In practice, sections 97, 97A, 97B, and 97C of the Bangladesh Telecommunication Regulation Act, 2001 provides the executive with overbroad legal bases to compel operator cooperation, while procurement of interception and monitoring systems has consolidated NTMC as a central data node. The result is a networked surveillance assemblage in which call-detail records and internet-usage logs are routinely funnelled to the state and enriched through linkages to identity and administrative datasets, even as precise authorization, retention, and audit rules remain opaque or under-specified. As indicated above, individuals with access to the intelligence-sharing platform operated by NTMC, or to other NID-linked databases, are known to have commercialized such access with limited risk of consequence due to weak oversight, fragmented accountability mechanisms, and the absence of credible enforcement.

At the core of this informal and/or unregulated information ecosystem sits the NID system, whose function as a universal identifier enables extensive cross-linkage across otherwise discrete datasets. As NID-linked information is routinely replicated, cached, or integrated across disparate servers operated by multiple public agencies, private vendors, and intermediaries, the identity infrastructure increasingly functions as a distributed ecosystem rather than a bounded system. In this configuration, a vulnerability, misconfiguration, or breach at any downstream node or replica can compromise the confidentiality and integrity of the broader identity network, allowing partial datasets to be recombined into comprehensive identity profiles. This fragmentation not only expands the technical attack surface but also diffuses responsibility across actors, complicating oversight, incident response, and remediation, and rendering the identity system structurally vulnerable to both inadvertent exposure and deliberate exploitation.

4.4 Sectoral laws without data-protection guarantees

Across major public bodies, ranging from the EC to BTRC and NTMC, data collection is usually enabled by sectoral statutes or licensing conditions. Yet, publicly accessible instruments rarely specify privacy fundamentals such as strict purpose limitation, retention and deletion schedules, secondary-use constraints, notice and consent mechanism, or independent redress. In consequence, legal mandates to collect and disclose data tend to be far clearer than the rules that would limit, regulate, or audit such processing.

For instance, the reportedly repealed National Identity Registration Act, 2023 and the National Identity Registration Act, 2010 empowers the EC to enrol and manage citizens' biometric and demographic data. While this statute classifies information stored in the NID infrastructure as confidential and criminalizes unauthorized access, disclosure, or use as non-bailable, cognizable offence, open-source research and interviews conducted for this study indicate that no enforcement action has been taken against any individual or entity, despite documented findings of irregularities against multiple public and private entities. However, the statute does not adequately address the broader issues around insider abuse, data-retention limits, restrictions on external sharing, or effective remedies for data subjects, and sector-specific guidelines or inter-agency agreements governing access and onward data sharing remain sparse or not publicly available.

Similarly, in the telecommunication sector, the Bangladesh Telecommunication Regulation Act, 2001, together with associated licensing regime, mandates confidentiality of customer information and prescribes punitive measures for violation, while simultaneously authorizing interception and compelling operator cooperation with law enforcement and intelligence agencies on broad public-order and security grounds, while imposing few transparent safeguards on targeting, retention, or oversight in practice. As a result, this regulatory structure results in limited and uneven data protection for customers and often enables state-sanctioned surveillance and monitoring.

For banking and financial services, statutory and prudential instruments, such as the Bank Companies Act, 1991, Financial Institutions Act, 2023, Bangladesh Bank Order, 1972, and downstream circulars and allied legislations like Anti-Terrorism Act, 2009 and the Money Laundering Prevention Act, 2012, require both customer due diligence, reporting, and monitoring to prevent illicit finance, while also ensuring customer confidentiality and secrecy. However, publicly available rules seldom detail post-purpose retention limits, secondary-use bans, or data-subject notification when information is shared with state agencies; supervisory instruments remain oriented to compliance and access rather than to privacy governance.

On November 6, 2025, the government introduced the Personal Data Protection Ordinance, 2025 and the National Data Management Ordinance, 2025. A central weakness of the framework lies in its expansive exemption carve-outs and broadly framed "necessity" provisions, which together risk rendering the statute largely unenforceable against public

operational protection. In practice, the critical-infrastructure designation has not translated into consistent preventive safeguards, timely detection, or credible enforcement, raising concerns about institutional capacity, accountability, and the deterrent value of criminalization in safeguarding citizens' most sensitive personal data.

Data vulnerabilities originating in the databases of NTMC and ORGBDR in 2023 are apt cases in point. Despite the nature and magnitude of these exposures, there was no meaningful, public-facing accountability: affected individuals were not notified through standardized breach disclosures, independently published forensic assessments were absent, and no clear sanctions or remedial actions against responsible units were made public. According to a government interviewee for this study, these shortcomings are only partly attributable to policy gaps; they are more accurately understood as an unintended byproduct of chronic institutional capacity constraints, including an overstretched and largely reactive e-Government Computer Incident Response Team operating without a clear or effective legal mandate. Another respondent observed that breaches are often treated by the government as operational anomalies to be absorbed rather than as systemic failures warranting structural reform, reinforcing an institutional environment in which accountability and organizational learning remain limited.

Across sectors, existing statutory frameworks, including the Births and Deaths Registration Act, 2004, the Passport Act, 1920, the Bangladesh Telecommunication Regulation Act, 2001, the Cyber Security Ordinance, 2025, and other sector-specific primary and secondary legislation, are ill-equipped to address contemporary data governance challenges or to regulate the informal marketplace for personal information that has emerged around NID-linked systems. While these laws authorize data collection, identity verification, and inter-agency cooperation for administrative, security, or regulatory purposes, they provide few binding rules governing secondary use, data retention and deletion, vendor access, or cross-sector data sharing. Instead, data sharing, aggregation, and reuse rely heavily on executive directions, informal coordination, and vendor-managed back-end systems, rather than on transparent and codified safeguards.

Overall, these statutory and regulatory frameworks create a data governance ecosystem in which both substantive and procedural legal protections function largely at a nominal or symbolic level, while state powers of access, control, and surveillance continue to expand. Across sectors, laws and licensing regimes clearly authorize data collection, disclosure, and cooperation with state authorities, yet provide only thin, fragmented, or weakly enforced safeguards governing purpose limitation, data retention, secondary use, and redress. Weaknesses at each layer of sectoral law and in their enforcement compound over time, rendering systemic vulnerabilities increasingly entrenched and institutionalized; and in a context characterized by weak, capacity-constrained, and often politicized oversight institutions, enforcement gaps — whether arising from institutional limitations or compromised regulatory independence — have allowed unregulated markets and informal commercial networks around personal data to persist and, in some cases, thrive. As a result, legislated privacy protections and accountability mechanisms remain largely aspirational, exposing citizens to heightened risks of misuse, unauthorized disclosure, surveillance, and downstream harm, particularly where public bodies remain among the largest collectors and aggregators of personal information.

4.5 Bureaucratic inertia, limited government expertise, and institutional dysfunction

A dominant theme across stakeholder interviews for this study was the pervasive bureaucratic inertia within state institutions tasked with data governance. While digital identity systems in Bangladesh have expanded rapidly over the last two decades, the corresponding regulatory and administrative frameworks have failed to evolve. Multiple interviewees, including legal, policy, and cybersecurity experts pointed to a critical lack of regulatory foresight, technical capacity, and operational readiness within key government agencies.

An interviewee formerly associated with the EC observed that there is limited institutional culture of data stewardship within the constitutional body, noting that no formal training on data protection, cyber hygiene, or ethical responsibilities were provided to data handlers, nor have standardized operating protocols for data handling been developed, from the earliest days of NID system implementation to the present As a result, staff routinely store sensitive data on unsecured devices and servers, personal email accounts, or unencrypted USB drives. Beyond internal practices, interview respondents familiar with the matter highlighted that this deficiency has had downstream effects, including the absence of robust data governance requirements and meaningful restrictions on onward data sharing in contracts executed with vendors and partner agencies, as well as a tendency to treat systemic data protection infractions by downstream actors as minor or inconsequential — reflecting a persistently low level of institutional data security awareness.

One key contributing factor is the absence of a sustained strategic investment in regulatory and technical expertise within the EC and other public institutions responsible for digital data governance. Decision-making authority over procurement, compliance, and inter-agency data sharing is frequently vested in politically appointed officials who often lack specialized understanding of complex digital systems and data governance practices, while also tending to treat such matters as low-priority policy issues. A combination of limited technical understanding and political pressure weakens effective oversight and ongoing risk assessment, while encouraging routine acquiescence to data-sharing requests from other state entities. As a result, in turn, these conditions create structural vulnerabilities conducive to regulatory capture, whether by private technology vendors with asymmetric expertise or by entrenched bureaucratic interests that privilege administrative convenience over accountability and rights protection.

Moreover, systematic auditing is neither a clear legal requirement nor institutionalized as a core component of bureaucratic practice. Where audits do occur, they are often ad hoc, reactive, and episodic, and are perceived less as tools for identifying systemic risk or strengthening institutional resilience than as mechanisms for managing political exposure, disciplining adversaries, or responding to media scrutiny. A compliance officer from a major mobile financial service provider interviewed for this study described regulatory audits as inconsistent in scope and methodology, marked by limited technical understanding of digital systems and data governance, and offering little guidance on standards, benchmarks, or follow-up actions. In the absence of clear policies, cybersecurity incidents are frequently followed by internal blame-shifting rather than structural or procedural reform, resulting in recurring vulnerabilities and limited organizational learning.

What is clear is that there is a lack of political will to enforce or institutionalize data protection norms. This is not simply a matter of legislative absence, but reflects deeper political, institutional, and incentive-driven dynamics that shape how data governance is understood and deprioritized in practice. These play out in four ways.

First, a state-first security paradigm prioritizes legibility and control over rights, consistent with neo-Weberian accounts of infrastructural power, Hobbesian order-maintenance, and securitization of NID and its infrastructure. Within this paradigm, citizens' data are treated primarily as instruments of governance, security, and administrative efficiency rather than as objects of rights-based protection. As such, investments that enhance access (such as centralized NIDs, interception, bulk verification) generate immediate utility for revenue, policing, and regime security; by contrast, investments in constraints (such as independent oversight, breach notification, deletion rules, redress systems) deliver diffuse, delayed benefits while imposing visible costs, procedural burdens, and friction on powerful agencies. In short, while the political return on control is high, the return on constraint is low, skewing the calculus in favor of greater and largely unregulated access.

Second, colonial and post-colonial administrative path dependence embeds a culture of command and exception, in which bureaucratic authority is normalized through directives and discretionary power, and legal limits on state action are subordinated to administrative or security imperatives. Bureaucratic repertoires inherited from census- and surveillance-centric governance models normalize exceptional access as routine, while legal frameworks rely on executive orders rather than justiciable limits. This legacy produces an administrative culture in which discretion is valorized and legal limits are viewed as operational inconveniences rather than binding obligations. In such settings, “compliance” often takes the form of isomorphic mimicry, with policies and contracts reflecting global best practices often lacking enforceable teeth. Formal alignment substitutes for substantive change. This helps explain why audits are episodic and instrumental (used for leverage or crisis management) rather than systematic risk assessment.

Third, contemporary political-settlement dynamics tie large information and communication technology procurements to rent and coalition management, meaning that government contracts and access to data infrastructures function as tools to distribute economic benefits and sustain political and bureaucratic alliances. Where long-term maintenance contracts and opaque vendor relationships double as tools of patronage, strong and independent regulators, adversarial oversight, and robust enforcement introduces uncertainty into “business as usual” in procurement processes and established arrangements that are politically valuable precisely because of their predictability and opacity. Agencies therefore face few internal rewards, and significant risks, for elevating privacy engineering, mandating per-user credentials and immutable logs, or enforcing breach reporting against peer bodies and favoured contractors. The result is a principal–agent inversion: vendors and security actors shape operational standards, while civilian regulators trail behind.

Fourth, transaction-cost politics skews institutional choices. Building a professionalized data-protection cadre, modernizing audit processes, and mandating privacy-by-design raises short-term costs for many actors (such as ministries, vendors, telecommunication service providers, banks) but brings long-term benefits to citizens as the ultimate beneficiaries. However, citizens are diffuse and weakly organized, and in the absence of constituencies capable of imposing sustained political or legal costs, privacy protection remains a low-salience issue. In the absence of inclusive policy co-creation with industry and civil society, an independent data protection authority, judicialized remedies, there is little countervailing pressure to shift that calculus. Consequently, the system defaults to ad hoc fixes, informal access, and retrospective denial — precisely the patterns observed in interviews.

Net result: government agencies frequently ignore or delay implementation of compliance frameworks, even when drafted in collaboration with industry, civil society, and other actors. Formal adoption does not translate into operational enforcement. The state often relies on the informal ethics or initiative of private actors to set minimum standards of protection. This is both unsustainable and dangerous, as this effectively privatizes public data governance and substitutes discretion for law, without durable institutional or legal anchors.

5. The role of private vendors

Over the past few decades, private vendors have become deeply embedded in Bangladesh's digital governance apparatus, in designing, maintaining, and operating core platforms that collect, process, and store sensitive citizen data. From a comparative perspective, this pattern aligns with global trends. Since the 1980s, New Public Management (NPM) reforms have encouraged governments to outsource non-core functions to non-state actors, and often rely on public-private partnership models like build-operate-transfer or design-build-finance-operate for complex technical systems and large-scale digital infrastructure development. In this light, Bangladesh's dependence on private vendors for digital identity, health, telecom, and other allied infrastructures appears as a pragmatic response to fiscal and capacity constraints, enabling the state to leverage specialist expertise and ensure rapid delivery through contractual controls.

Yet NPM-style outsourcing often externalizes not only implementation responsibilities but also critical design choices, governance assumptions, and risk allocation, enabling vendors to shape architectures, standards, and operational norms with limited public scrutiny. Decisions about system interoperability, logging, access controls, and data flows are frequently embedded at the design stage by private contractors rather than determined through public-interest-driven regulatory processes. In data-intensive domains, this can mean vendor-controlled back-ends, proprietary interfaces, and long maintenance contracts that lock in technical dependencies, limit state leverage, and raise switching costs, leaving public bodies poorly equipped, both technically and institutionally, to govern infrastructures they formally own.

Principal-Agent Theory clarifies how this dependence translates into power. Formally, the state is the principal and private firms are agents contracted to deliver specified services; however, in practice, persistent information asymmetries and weak contract-management capacity allow agents to accumulate discretion and agenda-setting influence well beyond their formal mandates. Technical vendors and telecom operators typically know far more than their public counterparts about configuration, logging, and integration pathways, placing them in a position to embed design choices at the outset that shape long-term governance outcomes, and thus effectively determine how access controls, data retention, and interoperability are implemented. Over time, long-term maintenance contracts, proprietary technologies, and vendor-managed back ends raise switching costs and limit the state's ability to monitor, discipline, or replace these agents, transforming formal delegation into de facto control. As a result, while legal ownership of digital infrastructure remains with public authorities, effective operational power migrates to private agents, constraining the state's capacity to impose stronger data governance, privacy protections, or accountability requirements ex post.

A network governance lens further underscores that these infrastructures are not purely “state” systems but state-market assemblages in which authority, expertise, and resources are distributed across ministries, regulators, vendors, donors, and other stakeholders. Such networks can foster innovation, but they also diffuse responsibility: when data leaks or misuse occur, each node can point elsewhere and no single actor has full visibility over the data lifecycle. Citizens, meanwhile, have little influence over these arrangements, while private actors enjoy contractually privileged access to critical databases and remain largely insulated from meaningful liability. Situating Bangladesh within these frameworks highlights that outsourcing and institutional embeddedness are part of a broader reconfiguration of state-market relations—and that, without deliberate counterweights, they tend to weaken traditional lines of public oversight, especially in high-stakes areas such as digital identity and electoral data.

Against this backdrop, the following section maps the contractual arrangements, infrastructural access, and accountability gaps surrounding these actors, to show how privatized data governance can erode transparency and public oversight.

> **Private vendors play a decisive, often under-scrutinized role in Bangladesh's digital governance, exercising de facto control over identity-linked infrastructures through technical expertise, backend access, and long-term contracts. Weak procurement safeguards, contractual opacity, and limited state enforcement capacity have shifted practical data governance from public oversight to vendor discretion, heightening risks of lock-in, unaccountable access, and data commodification.**

5.1 Vendors as de facto data controllers

A central feature of Bangladesh's e-governance strategy has been the outsourcing of technical infrastructure to domestic information technology firms. Companies such as Tiger IT Bangladesh Limited, Digicon Technologies Limited, Computer Network Systems Limited, and Synesis IT PLC have been contracted to design and operate core systems ranging from the NID architecture to biometric verification gateways.

Concerns about vendor power and state dependence have been amplified by reporting on large identity-linked projects. A 2025 investigation into the Bangladesh Road Transport Authority's (BRTA) smart driving licence system found that, more than a decade after launch, BRTA had never held full, independent control over its licence database or printing infrastructure. Instead, control over the server, database, and middleware was distributed across three contractors—Madras Security Printers Private Limited, Computer Network Systems Limited and Tiger IT Bangladesh Limited—with key printing functions ultimately dependent on remote authorization from Madras in India. After Tiger IT Bangladesh Limited was blacklisted by the World Bank for alleged corrupt and collusive practices in establishing NID system in 2019, BRTA cancelled its contract and appointed new vendors, but media reports indicate that the vendors did not promptly hand over server and database control, contributing to a prolonged disruption in card issuance and leaving roughly 1.25 million licence applications pending until mid-2021. Based on interviews with officials, vendors, and technical staff, the evidence suggests a pattern of vendor lock-in in which critical citizen databases and application layers remain practically, if not formally, under contractor control.

From a governance perspective, the BRTA case illustrates how weaknesses in procurement design, compounded by the absence of guiding frameworks and robust contractual safeguards, can translate into structural dependency. Reporting on the incident highlights that contracts did not guarantee immediate, verifiable transfer of source code, database credentials and operational control when vendors were replaced, nor did they embed strong sanctions for non-cooperation. As a result, restoring BRTA's control required a special intervention by the Information and Communication Technology Division, which had to reverse-engineer components and create workarounds to bypass external dependencies. While there is no public evidence that citizen data were deliberately tampered with or commercially exploited during the transition, it does not negate the possibilities; rather, the episode demonstrates how, in practice, the state's ability to exercise authority over its own identity-linked infrastructure can be constrained by contractual gaps, information asymmetries, and technical dependence on private actors.

A parallel set of concerns has emerged around the role of Digicon Technologies Limited in operating the Porichoy identity verification platform. Officially launched under the Bangladesh National Digital Architecture (BNDA) in 2019, Porichoy provides real-time NID-based verification services to banks, mobile financial service providers, telecommunication operators, and other public and private institutions.

One reporting indicates that the private vendor was entitled to an estimated 80-90% of the revenue from Porichoy transactions, effectively giving a private firm a large commercial stake in a state-backed identity gateway. By late 2024, the EC had revoked the BCC's access to the NID database, prompting the suspension of Porichoy and disrupting customer onboarding for downstream entities; legal analyses attribute this step to alleged violations of the underlying data-sharing agreement and ambiguities over how far NID data could be routed through private infrastructure. Again, the publicly available sources do not allege that Digicon Technologies Limited misused personal data, but they do reveal that a core identity verification service operated for years under arrangements whose legality and governance safeguards were later called into question.

Taken together, these cases do not prove a single narrative of intentional abuse by any one company. Rather, they point to a recurring governance pattern: critical identity-linked systems are architected, hosted, and maintained by vendors who possess superior technical knowledge, while state contracts lack clear provisions on data localization and control, source-code escrow, handover obligations, independent security audits, and sanctions for non-compliance.

For the purposes of this report, the core concern is not to adjudicate between competing claims about individual firms, but to show how these structural features of outsourcing and vendor lock-in can leave citizen data infrastructures vulnerable: formal ownership rests with public institutions, yet effective operational control, and hence much of the practical power over data, resides with private contractors who are only weakly embedded within public-law accountability frameworks.

5.2 Backend access and data commodification

The core risk posed by private contractors lies in their backend access to sensitive data. Generally, vendors operate or maintain the servers, databases, and APIs of government systems, giving them potential access to unencrypted personal data. In recent years, for example, Synesis IT PLC has built and operated platforms such as the Surokkha vaccine registration system and the Shastho Batayon telehealth line for the Ministry of Health and Family Welfare, and has also contributed to law-enforcement–facing analytics, including CCTV and interception-adjacent platforms. On the other hand, the NID infrastructure has been built, maintained, and operated by Tiger IT Bangladesh Limited since 2010, with reports indicating that the company continued in this role for at least seven years after the project's completion, and even after it was blacklisted by the World Bank amid findings of apparent patronage linked to the then ruling party. Computer Network Systems Limited reportedly took over parts of the NID infrastructure operations and maintenance thereafter and continues to provide services to the EC and other public entities.

Despite handling critical infrastructure, most contracts reviewed or described in stakeholder interviews lack explicit clauses on data retention, repurposing, anonymization, or breach penalties. The state apparatuses generally treat data as its property, but do not consistently translate this assertion of ownership into detailed, enforceable obligations governing how vendors store, log, back up, or delete that data. In practice, this creates room for contractors to retain full or partial copies of production databases for “operational” reasons (backups, staging, analytics), to subcontract components to third parties without clear flow-down restrictions, or to host datasets and logs on foreign cloud platforms. Stakeholders interviewed for this study expressed concern that such practices can blur jurisdictional lines and expose Bangladeshi citizens' data to foreign legal regimes and intelligence requests, particularly when vendors, suppliers, or hosting providers are based in countries with expansive surveillance powers.

A study mapping of surveillance procurement illustrates the scale of these vendor relationships. Procurement records and media investigations indicate that NTMC's Integrated Lawful Interception System (ILIS) was sourced from multiple foreign suppliers such as Yanna Technologies, Intersec, and Verint Systems, with NTMC officials repeatedly travelling to the United States for procurement discussions and vendor-led training. For other tools, public documents show that local firms act as systems integrators: for example, Tech Valley Solutions reportedly installed a deep packet inspection-based content-filtering system in Bangladesh using hardware imported from the United States, yet the manufacturer and model were not disclosed in public sources.

Each such arrangement potentially creates additional backend channels through which communications data, metadata, or derived profiles can be accessed, mirrored, or exported, with limited visibility for parliament, regulators, or affected individuals.

According to experts interviewed, in this environment, the absence of genuine, independent audits means vendors operate with very limited external scrutiny. Where present, ISO 27001 or similar certifications attest to the existence of an information security management system on paper, but hardly any steps are taken to continuously monitor day-to-day staff behaviour, consent practices, or unauthorized secondary uses of data. In concrete terms, this means that a system can be formally “certified” while copies of NID-linked logs remain on a developer's cloud bucket after a project ends, or while support teams use production datasets for testing and analytics in ways that were never made transparent to citizens. Without routine, technically competent third-party audits, on-site inspections, and the ability to compel disclosure of data-handling practices across entire vendor chains, risks such as silent data retention, cross-border replication, and function creep are likely to persist and compound—turning backend access into a central vector for commodifying and repurposing identity-linked data beyond the purposes for which it was originally collected.

5.3 Contractual opacity and regulatory gaps

Data-handling practices by vendors in Bangladesh are formally grounded in law, but only in indirect and partial ways. Public information technology and telecommunication projects are procured under the Public Procurement Act, 2006, as well as secondary legislations like the Public Procurement Rules, 2008 and Public Procurement Rules, 2025, and increasingly processed through the e-Government Procurement (e-GP) platform managed by the Bangladesh Public Procurement Authority (BPPA). These instruments require publication of tender notices and contract awards, and e-GP does improve visibility over who won which contract, at what price, and through which procedure. However, the substantive contracts themselves are rarely disclosed in full, and tender specifications are often curated in ways that effectively align eligibility criteria with the technical capacities or prior involvement of specific vendors. A study of public procurement and transparency in Bangladesh notes that while procedural openness has increased, detailed contract clauses often remain shielded by confidentiality provisions, commercial sensitivity, proprietary interests, security justifications, and exemptions under the Right to Information Act, 2009. This combination leaves the core legal terms governing data ownership, secondary use, and security largely invisible to citizens, watchdogs, and even other arms of the state.

Stakeholder interviews conducted during this study suggest that these arrangements are predominantly contract-driven, with procurement law providing only a broad, skeletal framework. As such, in principle, information and communication technology and telecommunication contracts could be structured to specify data ownership and purpose limitation, technical and organizational security measures, adherence to international standards, breach notification duties, independent third-party audits, and post-contract data destruction. In practice, however, stakeholders interviewed for this study—as well as comparative assessments of Bangladesh's procurement system—indicate that many contracts emphasize delivery timelines, pricing, and high-level service-level agreements, while leaving data-governance issues under-specified or couched in generic language. Where security requirements are mentioned, they frequently reference certifications (such as ISO 27001) or generic “best practices,” rather than enforceable, auditable obligations on logging, access segregation, retention limits, or deletion protocols. Because the full texts are not public, this picture necessarily relies on partial documents, interviews, and analogies to similar contracts in comparable contexts, an informational gap that is itself symptomatic of the broader accountability deficit.

The new Personal Data Protection Ordinance, 2025 is presented as a corrective to these gaps, but its capacity to reshape vendor governance remains uncertain. Civil society analyses note that while the statute introduces general principles of purpose limitation, data minimization, and consent, it also creates broad exemptions for state bodies on grounds such as national security, public order, and law enforcement, and leaves significant discretion to the executive to define additional exempt purposes. In its current form, the statute does not clearly integrate with the procurement regime—for example, by mandating standard data-protection clauses in procurement contracts, or by requiring that vendors processing government-held personal data be subject to independent inspections, certain restrictions, and meaningful sanctions. As a result, private contractors remain embedded in critical data infrastructures through contracts that are legally anchored but substantively opaque: they are bound by broad duties to deliver services and to cooperate with state requests, yet their concrete obligations around data retention, secondary use, cross-border transfers, and breach response are neither systematically specified nor publicly overseen.

5.4 Structural reliance on vendor goodwill for compliance

A key finding of this study is that government institutions in many cases are not enforcing compliance standards, even where they are codified in the contracts, often delegating enforcement action to vendors. This structural reliance on vendor discretion has, in practice, privatized core decisions around data security, access, and retention. As one contractor interviewed observed, vendors are often expected to “do the right thing”, rather than being held to explicit, enforceable standards.

This informal arrangement stems from two root causes: a lack of detailed legal instruments to mandate best practices and compliance, and limited state capacity to monitor and enforce compliance even where rules exist. Contracts reviewed for this study, as well as descriptions provided by interviewees, suggest that many government procurement contracts for information technology either entirely omit or weakly formulate clauses on data deletion and anonymization, granular access logging, incident response, and breach notification. Officials responsible for vendor oversight frequently lack the technical expertise required to interrogate system architecture diagrams, interpret security audit reports, or challenge vendor assurances. This creates a pronounced asymmetry in expertise and power: vendors are typically more technologically sophisticated than the regulators or procuring agencies that are meant to oversee them, and they operate mission-critical platforms—from NID verification APIs to health databases—with minimal independent checks.

Within this landscape, the incentives facing different private actors also diverge. Market-facing entities such as mobile network operators or major

sanctions, compliance risks remain largely self-declared.

6. Data exploitation, consent, and vulnerable populations

At the heart of Bangladesh's digital identity and data governance failures lies a disregard for meaningful consent, data minimization, and equitable treatment of citizens. Personal data is routinely over-collected, repurposed without disclosure, and exposed to misuse—conditions that disproportionately harm vulnerable populations. This section explores the implications of such systemic data exploitation, particularly for those interacting with the state through welfare systems, health services, or mandatory biometric registration.

> **Bangladesh's digital identity regime treats consent as a procedural formality rather than a substantive right, enabling routine data over-collection, mission creep, and opaque surveillance. These practices disproportionately harm vulnerable populations—welfare recipients, rural users, political dissidents, and patients—who face heightened risks of exclusion, profiling, and stigma with little transparency or redress.**

6.1 The fiction of informed consent

In theory, consent is a foundational principle of any rights-respecting data governance regime. In practice, consent mechanisms are virtually non-existent in Bangladesh's digital public infrastructure. For example, the NID registration process requires applicants to submit extensive demographic information and a full set of biometrics (fingerprints, iris scans, photograph, signature) as a precondition for obtaining a card that is now functionally indispensable for voting, banking, SIM registration and most public services. Officials interviewed and sample forms reviewed for this study emphasize eligibility criteria, required documents, and procedural steps, but do not explain in plain language how the collected data will be shared across agencies, how long it will be retained, or what rights applicants have to access, rectify, or object to processing. A similar pattern is visible in the e-passport application process, where online instructions focus on enrolment logistics and document requirements, while available public-facing materials say little about onward data flows between the Department of Immigration and Passports, the EC, law enforcement and intelligence agencies, and foreign border-control systems. In both cases, the individual is told what they must provide to receive a document, but not how their data will circulate once inside the state's systems.

Where privacy policies do exist in adjacent digital services, they often operate through broad deemed-consent clauses rather than specific, informed agreement. For instance, the Department of Social Services' website privacy policy states that the department will keep personal information confidential but may share "necessary data with other Government agencies and organizations," without specifying purposes, legal bases, or limits, and without offering any mechanism for objection or review. Such clauses are typically presented at a generic website level rather than at the concrete moment when a citizen fills out a form or submits sensitive details. In effect, the individual's continued use of the service is treated as blanket consent to wide, undefined inter-agency sharing, even though most users are unlikely to have read or understood these provisions, and have no realistic way to withhold agreement without losing access to essential services.

This approach makes "consent" largely illusory. From a rights-based perspective, and as defined in the Personal Data Protection Ordinance, 2025, a valid consent should be specific, informed, freely given, and revocable. By contrast, in Bangladesh's digital identity ecosystem, consent is often implied through mandatory forms or buried privacy notices, offered on a take-it-or-leave-it basis in contexts where refusal would mean exclusion from voting, welfare, communications, or cross-border travel. Deemed consent of this kind cannot credibly be considered informed consent. At the same time, it would be misleading to suggest that inter-agency data transfers are never justified: some degree of sharing between, say, EC and passport authorities is functionally necessary to prevent duplication or fraud. The problem, as this report contends, is that such transfers are currently normalized and expanded without clear statutory bases, transparent documentation, or user notification, and are retroactively covered by vague "consent" language rather than ex ante rules on necessity, proportionality, and oversight. This reinforces the broader thesis of the report: in Bangladesh's digital ID regime, consent operates more as a legal fiction that legitimizes expansive data circulation than as a meaningful safeguard of individual autonomy.

6.2 Data over-collection and mission creep

Across sectors, Bangladesh's digital systems collect and interlink large volumes of personal data, often far beyond what is transparently justified or effectively governed. Under both now reportedly repealed National Identity Registration Act, 2023 and National Identity Registration Act, 2010, the NID system, for instance, stores names, addresses, photographs, digital signatures, and ten fingerprints, and is increasingly used as a backbone for other systems. Similarly, SIM registration procedures that couple NID numbers with biometric verification, and health platforms such as Surokkha that link vaccination records and comorbidity information to NID entries, reflect practices that are broadly standard in many jurisdictions for purposes such as identity assurance, fraud prevention, and public health management. On their own, such linkages are not inherently problematic: public administrations legitimately require personal data to deliver services, target welfare, collect taxes, ensure national security, verify identities, and regulate markets.

The core concern, however, lies not in the existence of these linkages but in the absence of a clear governance architecture around them. Inter-agency data transfers and back-end integrations often take place without publicly articulated protocols, privacy standards, procedural safeguards, defined surveillance parameters, or robust measures to mitigate exfiltration and insider abuse. Immigration systems, for example, routinely process travel histories, biometric passport data, and visa records; NTMC and related surveillance infrastructures can then draw on telecom, identity, and border-control data to construct highly granular profiles. In principle, each of these domains can claim a legitimate mandate. In practice, the lack of explicit legal bases, purpose-specific limits, retention schedules, independent oversight, and rights of notification or challenge enables uncontrolled data flows and function creep.

These structural weaknesses are not abstract. A 2024 report by TechCrunch, based on an internal letter from the director of the NTMC to the Ministry of Home Affairs, describes how two senior officers from specialist policing units allegedly used their credentials on NTMC's national intelligence sharing platform to access "extremely sensitive" citizen information, including NID-linked identity details and call records, outside their operational remit and to pass those data to intermediaries on Telegram in exchange for payment. The episode illustrates how a centralized, deeply integrated identity and surveillance platform can be repurposed for private gain when granular access controls, real-time oversight, and effective deterrents are lacking. It also shows that function creep and over-collection do not only enable state overreach; they create parallel risks of opportunistic exploitation by insiders who can monetize citizens' data in informal markets.

From a data-minimization and purpose-limitation perspective, the obligations on public authorities differ from those on private firms that commercialize user data: states may justifiably collect certain categories of information for governance functions that private actors could not. Yet this does not exempt public systems from the need for proportionality and constraint. Even where data collection is necessary for voting, welfare targeting, or public health, clear boundaries are still required; for example, restricting reuse of vaccination data for policing, limiting immigration datasets from being repurposed for generalized intelligence, or ensuring that SIM-registration databases are not mined for unrelated marketing or profiling.

6.3 Disproportionate impact on the poor and marginalized

While all citizens are exposed to risks arising from data misuse and surveillance, the intensity and consequences of those risks are not evenly distributed. Citizens with greater financial resources, legal literacy, and social capital may sometimes mitigate or contest harms, but the risks are acutely higher for marginalized populations—those dependent on welfare, lacking legal literacy, or exposed to surveillance through discriminatory policing. These groups often have the least choice about whether to engage with digital systems and the least capacity to contest harm when things go wrong.

For instance, welfare beneficiaries must authenticate via NID to receive stipends or cash transfers, often through mobile financial services. When NID data are altered, exposed, or misused — for example, through misconfigured government payment platforms — recipients have little to no realistic recourse to recover missed payments or challenge unauthorized access. A typical scenario might involve an elderly widow whose social safety-net allowance stops arriving because her NID-linked record has been corrupted or frozen after a data incident; she is bounced between local offices, mobile money agents, and helplines, none of whom can explain or remedy the underlying data problem.

Rural and low-income citizens may use call centres such as 333 to query social services, where their personal queries are routed through private vendors operating the hotline infrastructure. If call recordings and metadata are reused for analytics, shared with third parties, or inadequately secured, users are unlikely to be informed and have little power to object. For instance, a farmer might call 333 to ask about food relief or dispute a local official's decision; his phone number, location, and the substance of his complaint could be logged on a vendor system and later used for unrelated outreach or profiling, without his knowledge or consent.

Political dissidents, ethnic minorities, and religious communities are especially vulnerable to profiling via NTMC's surveillance infrastructure and other security-led data systems. Combined data from telecommunication operators, passport databases, and social media monitoring can enable authorities to map association networks and movement patterns without judicial oversight or due process. A student activist who organizes protests on encrypted messaging apps, travels to meetings, and speaks to journalists by phone may find that, over time, these disparate traces are fused into a risk profile that triggers heightened scrutiny at checkpoints or visa interviews, despite no formal charge ever being brought.

Patients calling health helplines like Shastho Batayon may unknowingly disclose sensitive medical information that is recorded, transcribed, or analyzed by private vendors without any dedicated health-privacy protections. In a plausible composite example, a caller seeking advice about HIV status, mental health, or reproductive health speaks candidly to a telehealth operator, unaware that the conversation is being stored on third-party infrastructure with limited access controls; if those records were later accessed by non-clinical staff or exposed in a breach, the resulting stigma or discrimination could be severe.

These harms are often invisible. Without transparency obligations, people do not know when their data have been leaked, profiled, or repurposed. Breach notification is not practised, and effective redress mechanisms are essentially non-existent for most affected individuals. This asymmetry creates a structural imbalance in which powerful institutions, both public or private, face few consequences when things go wrong, while marginalized individuals experience the impact in the form of lost benefits, heightened surveillance, stigma, or quiet exclusion, often without ever understanding that the root cause lies in how their data were handled.

6.4 Psychological and political effects of surveillance opacity

The normalization of expansive surveillance infrastructure, without citizen knowledge or legal protections, fosters a culture of fear, silence, and mistrust. Citizens internalize the risk of being watched, profiled, or misidentified, particularly during interactions with law enforcement or administrative bodies. Political activists and journalists are especially cautious, aware that their communications and movements may be monitored through NID-linked systems. Tech Global Institute's mapping of cyber-surveillance in Bangladesh, for example, documents how interception and monitoring platforms procured for NTMC and other law enforcement and intelligence agencies allow the aggregation of call-detail records, location traces, and other metadata from multiple operators into central dashboards, and how a misconfigured Elasticsearch instance reportedly left such data exposed online. Even where no individual is directly targeted, knowledge that such systems exist, and that they can fail, can heighten feelings of vulnerability and self-censorship.

Such pervasive opacity erodes democratic participation and chills dissent. It transforms public infrastructure into a tool of social control rather than empowerment. As one interviewee put it, "the state's priority is unfettered access by any means, not the protection of our personal data." This reflects a broader governance ethos in which surveillance trumps accountability, and citizen agency is sidelined in favor of bureaucratic or security expediency.

7. Comparative global perspectives

As Bangladesh confronts the multifaceted challenges of digital identity governance, comparative insights from other national models offer vital guidance. This section examines regulatory and technical trajectories in India, the European Union, Australia, Singapore, and China. Together, these cases represent a spectrum, from rights-respecting, consent-based architectures to surveillance-heavy, state-dominated frameworks. They provide not only policy inspiration but also urgent warnings about the risks of unchecked data centralization.

> **Comparative global models show that digital identity systems can either enhance citizen control or entrench surveillance, depending on consent design, legal safeguards, and institutional oversight. Experiences from the EU, Singapore, Australia, India, and China underline that without enforceable rights, independent regulators, and strict vendor governance, centralized identity infrastructures risk sliding toward opaque data extraction and authoritarian misuse.**

7.1 India's Aadhaar: centralization, consent, and surveillance risks

India's Aadhaar system illustrates the tension between scale, administrative efficiency, and civil liberties in national digital ID schemes. Initially justified as a tool to streamline welfare delivery, Aadhaar rapidly expanded into a de facto national identifier used for banking, telecommunication, taxation, and a wide range of public and private services, prompting concerns about mission creep and function sprawl. In its 2018 judgment in Justice K.S. Puttaswamy (Retd) v. Union of India, the Supreme Court upheld Aadhaar in principle but imposed important guardrails: it struck down section 57 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 to prevent private entities from demanding Aadhaar without a specific legal basis, curtailed mandatory linkage to bank accounts and mobile numbers, and read down provisions that had allowed retention of authentication logs for five years, limiting Unique Identification Authority of India (UIDAI) to six months. These rulings helped catalyze technical and policy adjustments such as the introduction of virtual IDs and revisions to authentication regulations, which were framed as measures to reduce the risks of pervasive tracking and profiling via a single identifier.

Yet substantial gaps remain in Aadhaar's accountability architecture. UIDAI continues to exercise operational control over core infrastructure and standards while also functioning, in effect, as a self-regulator. Critics argue that such concentration of technical and regulatory power, combined with mandatory logging of authentication events and wide scope for database linkages, sustains structural surveillance risks even under a more constrained legal regime. Vrinda Bhandari and Renuka Sane's A Critique of Aadhaar Framework explicitly contends that Aadhaar's institutional design leaves the accountability framework "weak", with limited independent oversight, unclear liability chains, and inadequate remedies for individuals adversely affected by exclusion, misuse, or data breaches

For Bangladesh, Aadhaar's evolution offers several concrete lessons. First, large-scale technical deployment should not outpace the development of a robust legal framework: once an identifier becomes foundational for welfare, finance, and telecommunications, retrofitting privacy and accountability is politically and technically much harder. Legal rules on purpose limitation, functional separation (for example, between civil registration, welfare targeting, and law enforcement), and data minimization need to be designed alongside, not after, system architecture. Second, independent oversight must be baked into institutional design from the outset. India's experience shows that placing both operational control and standard-setting within a single authority can weaken checks and balances; Bangladesh should ensure that any future data protection authority, sectoral regulators, and audit bodies have real powers over various private and public digital ID operators and aggregators, rather than leaving them in a UIDAI-like position of self-regulation. Third, transparency and public contestation are essential: publication of data-protection impact assessments, authentication and access statistics, and clear procedures for redress can help prevent the entrenchment of opaque practices that are difficult to reverse later. Finally, Aadhaar underscores that vendor governance and backend control are not technical footnotes but central to rights protection; Bangladesh will need explicit statutory and contractual controls over private implementers of NID-linked systems if it is to avoid replicating the same mix of large-scale dependence, limited scrutiny, and unresolved vulnerabilities.

7.2 European Union's GDPR: rights, redress, and accountability

The European Union is widely regarded as a leading reference point for rights-based digital identity governance. Its guiding philosophy is the digital sovereignty of the individual—"everyone should retain meaningful control over their own digital identity data".

All digital ID schemes in the EU operate within the framework of the General Data Protection Regulation (GDPR), which mandates a lawful basis for processing, data minimization, purpose limitation, privacy by design and by default, and enforceable rights to access, rectification, erasure, restriction, objection, and portability. Building on this foundation, the proposed European Digital Identity Wallet is designed to enable selective disclosure (for example, proving that a person is over 18 without revealing their full date of birth) and to allow consent for data use to be revoked in a granular and operational way.

What distinguishes the EU model is not only the legal text but also its institutional architecture. Every member state must maintain an independent Data Protection Authority (DPA), and large-scale controllers and processors are required to appoint internal Data Protection Officers (DPOs). These bodies are empowered to investigate, issue binding orders, and impose substantial fines. A practical illustration is France's Alicem digital identity app: when it relied on mandatory facial recognition, the French DPA raised concerns that the scheme did not offer a genuine alternative for those unwilling to undergo biometric processing, pushing the government to adjust its approach to align with GDPR's standards on consent and voluntariness. More broadly, the Court of Justice of the European Union has repeatedly invalidated measures, such as blanket data-retention regimes, that it deemed incompatible with fundamental rights, signalling that digital identity and data infrastructures remain subject to robust judicial review.

For Bangladesh, the EU experience offers a normative blueprint: consent should be meaningful in practice rather than formal, oversight must be institutionally independent, and data handling needs to be transparent, auditable, and open to challenge. However, it also underlines an important caveat: well-drafted legislation is not sufficient on its own. GDPR's relative effectiveness rests on decades of institutional development, sustained investment in regulatory capacity, and a political culture that tolerates regulators and courts ruling against executive preferences. Without parallel reforms—such as building independent supervisory bodies, clarifying mandates, resourcing enforcement, and protecting whistle-blowers—even the most carefully worded data protection statute in Bangladesh risks remaining largely symbolic. Adopting GDPR-inspired principles of proportionality, clear legal bases for processing, and opt-out or objection rights is therefore necessary but not sufficient; these must be coupled with credible institutions capable of enforcing those principles against both state and private actors.

7.3 Australia's PSPF: vendor governance and system security

Australia's Protective Security Policy Framework (PSPF) offers a useful reference point for thinking about how to secure government data infrastructures that depend heavily on private vendors. It sets mandatory protective security outcomes for Commonwealth Government entities and now explicitly links information security, third-party risk, and data sovereignty, with agencies encouraged or required to use certified providers (for example, under the Hosting Certification Framework) or to conduct structured risk assessments that address where data is stored, who can access it, and how incidents will be handled. Contracts for systems that handle sensitive personal information, including digital-identity–related data, are typically expected to reference the Privacy Act 1988 and PSPF obligations, with clauses on audit rights, notification duties, and, in some cases, on-site inspections and termination for security breaches. In other words, vendor management is treated as a security function, not just a procurement issue.

The Optus breach in 2022 is now a canonical case illustrating how this framework is supposed to work in practice when something goes wrong. The incident involved unauthorized access to the personal data of about 9.5 million current and former customers—roughly 40% of the Australian population—including passport and driving-licence numbers, addresses, and contact details. In response, the federal government rapidly activated cross-agency measures (for example, temporary rules to support document replacement and enhanced fraud monitoring), while the privacy regulator, the Office of the Australian Information Commissioner (OAIC), opened a formal investigation and has since initiated civil penalty proceedings, alleging that Optus failed to take "reasonable steps" under the Privacy Act 1988 to protect personal information from misuse and unauthorised access. Parallel class actions and investigations by the communications regulator have reinforced the idea that serious lapses in data security will attract regulatory, legal, and reputational consequences.

Underlying this is a broader legal architecture. The Privacy Act 1988 and the Australian Privacy Principles (APPs) impose baseline duties on agencies and covered companies: providing notice about data use, limiting secondary purposes, ensuring data quality and security, and giving individuals avenues for complaint and redress through the OAIC. The Notifiable Data Breaches (NDB) scheme adds a specific obligation to notify both affected individuals and the OAIC when a breach is likely to result in "serious harm", creating a structured process for disclosure and remediation and ensuring that large incidents, such as the Optus case, cannot be dealt with quietly. For Australia's emerging digital ID framework, additional obligations sit on top of these general rules, including more granular breach notification and privacy-impact assessment requirements for accredited entities.

For Bangladesh, the lesson is less that Australia has a flawless model and more that security and vendor governance have been treated as core elements of the regulatory field, not as afterthoughts. Three points are particularly salient. First, procurement and accreditation can be used to hard-wire minimum security and privacy baselines into vendor relationships (for example, clear allocation of responsibility, auditability, and post-contract data destruction), rather than relying on informal expectations of good behaviour. Second, breach-notification and enforcement mechanisms—anchored in a reasonably independent regulator—create both incentives to invest in security ex ante and a structured pathway for remediation and public communication ex post. Third, even with these mechanisms, the Optus case shows that serious failures still occur; what distinguishes the Australian response is that they triggered visible regulatory action, parliamentary scrutiny, and material consequences for the firm, rather than being normalized as business as usual.

For a context like Bangladesh, where vendors often enjoy extensive backend access with limited oversight, these examples suggest that legal reform around data protection will only be meaningful if it is accompanied by parallel investment in procurement standards, supervisory capacity, and enforceable contractual templates that make security, transparency, and redress non-negotiable in public–private data infrastructures.

7.4 Singapore: identity assurance and vendor accountability in NDI

Singapore's National Digital Identity (NDI) ecosystem, centred on Singpass and the Myinfo data-sharing service, is often cited as a relatively high-trust model of digital identity governance. Singpass provides a single authentication layer for both public and private services, while Myinfo enables pre-filled forms using verified data drawn from government sources, but only after the user has explicitly consented to each transaction. Consent is granular and event-based: when a bank or platform wants to retrieve specific attributes (for example, name, address, income band), the user sees a clear screen listing the exact fields requested, approves or declines, and the transaction is logged. This architecture, together with the fact that relying parties can integrate only via GovTech-managed APIs and the APEX exchange, limits informal data flows and keeps a central audit trail of which organization accessed what, when, and on what declared basis.

Singapore's handling of pandemic tools illustrates how this technical design is coupled with responsive governance. When it emerged that TraceTogether contact-tracing data could be accessed by police under the Criminal Procedure Code 2010, despite earlier assurances to the contrary, public backlash forced the government to introduce a specific statutory amendment limiting such access to a narrow set of serious offences and codifying safeguards. While the broader political context remains state-centric, this episode shows a willingness, at least in high-salience cases, to recalibrate legal rules in response to public concern and to acknowledge that repurposing digital tools beyond their original scope requires explicit legal justification and constraints.

For Bangladesh, several lessons follow from the Singapore experience, even allowing for very different institutional and political conditions. First, consent has to be designed as a real, operational control: every major identity-linked transaction should be mediated through a state-controlled gateway that presents users with intelligible, transaction-specific prompts and produces user-visible logs, rather than relying on one-off deemed consent buried in forms. Secondly, all public and private actors should access core registers (such as NID) only through standardized, centrally governed APIs, with GovTech-style technical baselines (mutual authentication, logging, least-privilege access) and contractual obligations; point-to-point database exposure and ad hoc data exports are precisely what Singapore's NDI stack is designed to avoid.

Singapore's trajectory shows that even in a strong, security-oriented state, public pushback can force clearer legislative limits on data repurposing. For Bangladesh, this suggests that building channels for civil society, media, and courts to contest mission creep in digital ID systems is as important as the initial system design. Singapore underlines that inclusion and protection can be pursued together through accessible interfaces, delegated or assisted consent, and user education, but only where there is sustained institutional discipline and clear governance mandates; transplanting interface features without parallel investment in oversight and accountability would risk reproducing the appearance of consent without its substance.

7.5 China: surveillance-heavy model and governance risks

At the authoritarian end of the spectrum, China exemplifies digital identity systems oriented toward state control, minimal transparency, and pervasive surveillance.

In China, the national identity infrastructure is tied into every domain, including banking, telecommunication, healthcare, and online activity. Recent proposals for a unified digital ID for internet users would effectively eliminate online anonymity. Although China passed a Personal Information Protection Law in 2021, broad carve-outs for state agencies mean

European Union	GDPR enforcement	Rights-based law and independent oversight are essential.
Australia	Secure vendor governance	Procurement and vendor control are critical risk points.
Singapore	Consent-based, auditable NDI	Strong design, transparency, and user control build trust.
China	Totalizing surveillance via ID	Without checks, identity systems become tools of repression.

For Bangladesh, these models offer both blueprints and warnings, and the imperative is clear: any digital identity system must be anchored in consent, purpose limitation, legal safeguards, and citizen control. Without these, the infrastructure built to serve the people risks being turned against them.

8. Reform recommendations

The preceding analysis shows that Bangladesh's digital identity and data governance regime is not broken at a single point but fragmented across laws, institutions, and infrastructures. Fixing one element in isolation—for instance, tightening NID access—will not be sufficient if supply chain, surveillance powers, and institutional and enforcement capacity remain unchanged. The non-exhaustive recommendations below therefore focus on a small set of structural priorities that should be implemented in a phased and adaptive manner, recognizing that regulatory coherence, institutional accountability, and technical capacity must evolve together.

> **Effective reform of Bangladesh's digital identity ecosystem requires systemic change—coherent inter-agency data governance, independent oversight, enforceable vendor controls, and legally bounded surveillance powers. Without operational consent, breach notification, and real remedies for citizens—especially vulnerable groups—legal reforms risk formalizing opacity rather than restoring accountability and trust.**

8.1 Build a coherent state data governance architecture and formal inter-agency rules

A first priority is to move from ad hoc, bilateral data-sharing practices to a coherent, legally grounded data governance architecture. At present, intra-state data flows are driven by informal arrangements, executive orders, and opaque technical integrations. Bangladesh should adopt a clear framework—whether through a revised National Data Management Ordinance, 2025 or a standalone public sector data governance statute that: (a) defines the legal bases and purposes for inter-agency data sharing; (b) requires written, publicly accessible data-sharing instruments (memorandum of understanding, service agreements, or regulations) for all systematic exchanges; and (c) mandates a central register of high-risk data flows (e.g. NID–telecom, NID–immigration, NID–law enforcement) with summaries available to the parliament and, in anonymized form, to the public.

Such a framework should also clarify institutional mandates. Rather than leaving coordination to personalities and informal committees, it should assign explicit responsibilities for data stewardship, interoperability, and privacy impact assessment to specific bodies (for example, a reconstituted and more independent national data authority) and require that new digital systems undergo ex ante impact assessments where they connect to core identity infrastructure. This would begin to replace the current "network of convenience" with a governed architecture in which inter-agency coordination is documented, reviewable, and contestable.

The Personal Data Protection Ordinance, 2025 and National Data Management Ordinance, 2025 represent an important acknowledgment that Bangladesh needs modern data governance laws. However, as noted earlier, their current form reflects an ambitious but under-designed framework: extraterritorial provisions that risk overreach; expansive exemptions for state authorities; broad executive discretion over rules and classifications; disproportionate criminal penalties; individual liability provisions that invite "hostage-taking"; and the absence of a realistic implementation roadmap.

Before these ordinances are fully operationalized, they should be subject to a structured revision process, with transparent public consultations and detailed, published drafts. Key amendments would include narrowing extraterritorial scope to situations with a clear nexus to Bangladesh; replacing open-ended state exemptions with tightly defined, necessity- and proportionality-tested grounds subject to independent oversight; constraining executive rule-making through clear statutory criteria and procedural safeguards; recalibrating penalties towards proportionate, primarily administrative sanctions; and clarifying the relationship between these statutes, sectoral laws, and existing secrecy or security statutes. Without such reforms, there is a serious risk that the ordinances will entrench the opacity and impunity documented in this report, while remaining under-enforced where accountability is most needed.

8.2 Create independent oversight, breach notification, and a statutory right to compensation

Bangladesh's current framework lacks an independent authority with the mandate and capacity to audit state and private actors, investigate breaches, and provide redress. A re-designed data protection authority should be established on genuinely independent footing, with transparent appointment processes, secure tenure, and guaranteed budgetary allocations. Its powers should include the ability to conduct proactive audits; issue binding codes of practice; order the suspension of high-risk processing; require privacy impact assessments for systems such as NID infrastructures, NTMC's intelligence sharing platforms, and Postal Vote BD, the expatriate voting app, and impose proportionate administrative penalties.

Alongside institutional oversight, individuals need enforceable remedies when things go wrong. A statutory breach-notification regime should obligate both public bodies and vendors to notify the authority and affected individuals where a breach is likely to result in material risk of harm, and to publish anonymised summaries of significant incidents. In addition, the government should introduce a clear statutory right to compensation for material harms arising from serious privacy violations, drawing on comparative models such as California Consumer Privacy Act of 2018 (which provides fixed-range statutory damages per affected individual for qualifying data breaches) and Australia's new statutory tort for serious invasion of privacy in Schedule 2 of the Privacy Act 1988, which sets structured parameters for non-economic loss.

Crucially, the design of such a scheme must include objective criteria for assessing harm, reasonable ceilings and floors, and procedural safeguards to avoid purely symbolic awards or punitive over-reach. The point is not to trigger a wave of litigation but to create a credible, predictable remedy that aligns incentives for both public and private actors to invest in prevention.

8.3 Standardize and open up vendor and telecommunication governance

Contractual vendors and private telecommunication operators currently sit at the heart of Bangladesh's digital identity infrastructure, but the contracts and licensing instruments that govern their access to citizen data are largely opaque. Existing frameworks, including procurement and telecommunication laws, focus on process (tenders, bids, awards via e-GP, or licensing and revenue-sharing) rather than on the substance of data-handling obligations, while confidentiality clauses and national-security exemptions often shield contracts from public scrutiny. This study suggests that, in practice, many of the most consequential decisions about data retention, replication, and backend access are effectively delegated to third party non-state actors with commercial interest in the data.

Reform in this area should proceed on three fronts. First, Bangladesh should develop standardized contract templates for all government information and communication technology and data-processing procurements, incorporating non-negotiable clauses on data ownership, purpose limitation, role definition (controller or processor), security baselines, encryption, localization and cross-border transfer, subcontracting limits, audit rights, incident reporting, and post-contract data destruction and handover. These templates should be mandatory, with limited room for derogation, and aligned with the legal frameworks.

Second, non-sensitive portions of vendor contracts and telecommunication licences and executive directions—particularly those concerning data handling and security—should be proactively published, with clear explanations in plain language. This would allow the parliament, judiciary, civil society, and the media to scrutinize whether terms match official privacy rhetoric, and would help normalize the idea that data-governance obligations are a matter of public interest, not solely commercial negotiation.

Third, telecommunication licensing and regulatory guidelines (covering mobile network operators, internet service providers, internet gateways and exchanges, and other network actors) should be revised to ensure that obligations to facilitate lawful access are balanced by explicit duties to minimize collection, restrict retention, log and justify disclosures, and support user rights. At present, these instruments are heavily skewed towards security access; recalibration is needed so that the same legal texts that authorize surveillance, interception, and data access by state actors also codify safeguards, oversight, and user protections.

8.4 Invest in institutional capacity, internal controls, and bureaucratic culture

A recurring theme in this study is the gap between technological ambition and institutional preparedness. Many of the governance failures documented here stem not only from legal gaps but from weak technical capacity, minimal data-stewardship training, and an administrative culture in which audits, logs, and privacy impact assessments are seen as burdens and non-essential obligations rather than core responsibilities.

Reform therefore requires sustained investment in people and processes. Key agencies in the digital identity and surveillance chain should be required to establish internal data-protection and cybersecurity units, staffed with qualified professionals, and to appoint data protection officers with clear mandates and reporting lines. Routine practices such as role-based access control, joiner–mover–leaver procedures, tamper-evident logging, and regular third-party security assessments need to be standard, not exceptional.

Equally important is cultural change. Training programmes should move beyond checklists to engage with ethical, legal, and political dimensions of data governance, including how mission creep, informal look-ups, and "helping out" other agencies can cumulatively undermine rights. Internal performance metrics and incentives should reward good data stewardship rather than mere throughput. Without this institutional groundwork, even well-designed laws and contracts will remain under-implemented.

8.5 Re-balance surveillance and security powers with legality, necessity, and proportionality

The legal framework underpinning NTMC and related interception and monitoring powers—anchored in provisions such as sections 97 and 97A–C of the Bangladesh Telecommunication Regulation Act, 2001—currently provides a broad statutory hook for pervasive surveillance, but without the detailed implementing rules, independent authorization procedures, and oversight mechanisms that rule-of-law standards require. As case studies in this report illustrate, this has enabled large-scale aggregation of NID-linked metadata, occasional technical leaks, and, in some instances, insider abuse and unauthorized resale of classified data, all with limited public explanation or accountability.

Reform here should focus less on abolishing surveillance capacity and more on embedding it within a framework of legality, necessity, and proportionality. This would entail: codifying clear thresholds and purposes for interception and bulk data access; introducing independent or judicial authorization for high-risk requests; setting retention limits and deletion requirements for different data categories; requiring detailed, tamper-evident audit logs for all accesses; and mandating periodic, published transparency reports on aggregate surveillance activity. Where security agencies rely on vendor-supplied systems, contracts should explicitly prohibit secondary use, export, or cross-border sharing of data beyond specified channels, and subject these systems to regular technical and legal audits. The aim is to ensure that surveillance operates as a bounded tool under law, not as an open-ended infrastructure of control.

8.6 Make consent, user rights, and protection of vulnerable groups operational in high-risk systems

Finally, the report has shown that consent and user rights are largely aspirational in the current ecosystem: NID, passports, SIM registration, health platforms, and welfare systems demand extensive personal data as conditions for participation, but offer little by way of explanation, choice, or recourse. This is particularly acute for people who are dependent on state services, lack legal literacy, or are at heightened risk of profiling and discrimination.

Reform should therefore prioritize making consent and user rights operational in the systems that matter most. Concretely, this means redesigning key forms and digital interfaces (NID registration, passports, welfare enrolment, health and helpline platforms, and new electoral tools such as Postal Vote BD) to include clear, accessible explanations of what data are collected, for which purposes, which agencies will receive them, how long they will be kept, and how individuals can exercise rights of access, correction, and complaint. It also means building user-facing access logs—"who looked at my record, when, and under what legal basis"—for core identity systems, with special support channels for low-income, rural, or otherwise marginalised users.

In parallel, specific safeguards should be introduced to prevent sensitive datasets (such as health records, welfare beneficiary lists, and telecom metadata) from being repurposed for law enforcement, political profiling, or commercial targeting without clear statutory authority and independent review. Here, comparative experiences—from Aadhaar's post-litigation guardrails to EU-style data-subject rights and Singapore's granular consent mechanisms—offer both cautionary tales and constructive models. The central lesson is that digital identity systems can support inclusion and service delivery only if they also embed enforceable limits on how identity-linked data are used, shared, and monetised.

9. Conclusion

This paper has mapped Bangladesh's digital identity ecosystem as an increasingly networked infrastructure in which the NID functions as a common identity spine across public administration, regulated markets, and security institutions. Rather than operating as isolated sectoral databases, systems in telecommunications, health, immigration and border control, social protection, and finance are increasingly connected through NID-based verification and shared identifiers. This interconnection expands the utility of digital services, but it also amplifies systemic risk: exposure, misuse, or weak governance in any downstream node can cascade across domains as fragmented records are recombined into comprehensive profiles.

The core finding is that Bangladesh's current governance regime enables data-intensive governance without commensurate safeguards. Interoperability has expanded through a mixture of formal integrations and commercially mediated access pathways, yet purpose limitation, retention rules, breach notification, and meaningful redress remain under-developed or unenforced. Sectoral laws and administrative practices frequently facilitate collection and linkage, while offering limited protection against repurposing, unauthorised disclosure, or commercial exploitation.

A particularly consequential dynamic is the role of private vendors and intermediaries as de facto data controllers. Across identity, health, and security-linked infrastructures, contractors frequently build, host, and maintain core systems, creating conditions for backend access, vendor lock-in, and opaque accountability. Even where misconduct is not proven, the governance pattern is structurally risky: when the state relies on vendor goodwill rather than enforceable technical and contractual controls, public responsibility for data stewardship is effectively delegated to actors without democratic accountability.

The paper also shows how identity infrastructure has become entangled with surveillance capacity. Telecommunications governance and interception powers, consolidated through institutions such as NTMC, illustrate how data linkages enable a 'surveillance assemblage' that fuses identity, communications metadata, and other administrative traces. In the absence of clear implementing rules, independent authorisation, robust auditability, and credible deterrence against insider abuse, such systems create risks of both state overreach and opportunistic exploitation of sensitive data in informal markets.

These dynamics produce uneven harms. Citizens with fewer resources and less institutional power are more likely to be compelled into data-intensive procedures, less able to refuse collection, and less able to contest errors or misuse. For marginalized groups and politically exposed communities, opaque surveillance infrastructures can generate chilling effects, inhibit civic participation, and deepen mistrust in state institutions.

The reform agenda proposed in this paper responds to these structural problems rather than treating breaches as isolated technical failures. It calls for: a coherent state data governance architecture with formal inter-agency rules; an independent oversight body with audit powers, breach notification obligations, and a statutory right to compensation; standardized vendor governance and procurement transparency; sustained investment in institutional capacity and internal controls; proportionate, legally bounded surveillance; and operational consent, notice, and protections for vulnerable groups.

Ultimately, what is at stake is the legitimacy of Bangladesh's digital state. Digital identity can support inclusion and efficient service delivery, but only if it is governed as a rights-bearing public infrastructure rather than an extractive, security-led assemblage. Embedding transparency, accountability, and citizen agency into identity systems is therefore not a peripheral 'privacy' concern; it is a foundational condition for democratic accountability, digital sovereignty, and data justice in Bangladesh's ongoing transformation.