

<https://doi.org/10.59298/NIJEP/2026/6111000>

Digital Identity Systems: Privacy, Access, and State Capacity Outcomes

Kabiga Chelule Kwemoi

Faculty of Engineering Kampala International University Uganda

ABSTRACT

Digital Identity Systems (DIS) have emerged as transformative infrastructures that reshape interactions between citizens and the state by influencing access to public services, privacy protection, and governmental capacity. This study examines the relationship between Digital Identity Systems and three interconnected outcomes: privacy, accessibility, and state capacity. It explores how the design, governance structures, and implementation strategies of DIS determine their ability to promote inclusive service delivery while safeguarding individual rights. Drawing on comparative perspectives from countries including Kenya, Nigeria, South Africa, Tanzania, Uganda, India, and other global contexts, the study highlights variations in digital identity approaches and their implications for governance. While DIS can enhance administrative efficiency, reduce fraud, improve accountability, and expand access to essential services, they also create significant risks related to surveillance, data misuse, exclusion, and weakened individual autonomy. The analysis demonstrates that effective digital identity governance requires balancing state interests with citizens' privacy rights through strong regulatory frameworks, transparent data practices, inclusive design, digital literacy initiatives, and accountable oversight mechanisms. The study argues that Digital Identity Systems should not be evaluated solely as technological tools but as socio-political infrastructures that influence state-citizen relationships. Sustainable and equitable digital identity ecosystems depend on privacy-preserving architectures, interoperability, citizen empowerment, and policies that address inequalities in access and participation.

Keywords: Digital Identity Systems, Privacy and Data Governance, Digital Inclusion, State Capacity, and Citizen Access and Accountability.

INTRODUCTION

Digital Identity Systems (DIS) constitutes the embodiment of a socioeconomic contract between citizens and governments and represent a key social distinction lacking access to public services. Digital Identity Systems (DIS) are defined as a set of data management processes and governance agreements that digitally, securely, and uniquely verify a citizen's identity for civic engagement with a relevant government [1]. In Africa, the impact of Digital Identity Systems on state capacity, privacy, and access to services is critical. Comparative policy analysis across multiple domains of investment and implementation reveals considerable variability among national Digital ID systems, affecting their outcomes [2]. Selected cases spanning varied ambitions, governance structures, and institutional objectives draw out these influences: [1] Kenya implements a comprehensive, cross-sectoral system aimed beyond public service delivery; [2] Nigeria pursues an expansive biometric ID focus, complemented by financial inclusion efforts; [3] South Africa's user-free, multi-purpose mechanism unduly restricts matriculatory and mobility services; [4] Tanzania's multi-modal, portable ID emphasizes domestic, infrastructural access; and Uganda's selective, integrated platform concentrates on emergency and social rights [1]. Beyond geographical contexts, systematic differences in policy design and functional articulation shape the interaction of Digital Identity Systems (DIS) with state capacity, privacy, and access [1]. The selected countries like Kenya, Nigeria, South Africa, Tanzania, and Uganda, bolster purposive contrast across regimes in Africa's historically low Digital Identity System (DIS) coverage. Privacy dimensions encompass data minimization, consent, control, and autonomy; access

NIJEP Publications

dimensions comprise inclusion, digital literacy, barriers, and interoperability; state capacity dimensions link to administrative efficiency, fraud prevention, and accountability [2]. These three underpinning criteria jointly constitute the analytical framework analyzing DIS for their aggregate effect on citizen engagement with government and hence on state capacity capabilities and services. Policy-relevant findings pinpoint conditions conducive to each of the three outcome dimensions, contributing both conceptual clarity and practical insight across a continent [2]. African nations rank lowest among all world regions in both general and biometric coverage of Digital Identity Systems (DIS) whole. Digital Identity Systems (DIS) span various data-collection modalities including biometric, biographical, documentary, digital, health, knowledge-based, and payment methods. The coverable outcomes of Digital Identity Systems (DIS) comprise state capacity, privacy, and access [2]. State capacity enshrines the diverse governmental capabilities and public service provisions available to a citizen. Digital access embraces the range of connectivity and functionality available on the digital Internet via public online services. Privacy characterizes the relative safeguarding of one's identity in the public realm and digital sphere [3]. Public services administered by governmental authorities represent standard procedures for accessing capabilities and deliverables pertaining to a given Digital Identity System (DIS). The vernacular usage of the term capability specifically references the aspirational achievable from public interactions with governmental agencies [4]. Governments commonly find themselves in a dilemma concerning Digital Identity Systems (DIS) due to the digital revolution. Digital Identity Systems (DIS) convey the dual prospective of augmenting government capabilities through efficiency while simultaneously posing a material threat to civil liberties, enhancing the potential for repression [2]. All governments must grapple with striking an appropriate policy balance encompassing the aforementioned trade-off. Addressing and ameliorating this challenge form the motivation behind a high-profile series of ID4D conferences promoted by the World Bank. Identification constitutes the fulcrum of social contracts governing assertable rights, binding individuals and nation-states within a defined jurisdiction [3]. The fulcrum is further pluralized through differentiation into Personal Identity and Legal Identity. Personal Identity is defined as self-perception with self-ascribed personal identifiers whereas legal identity signifies those identity elements recognized by the courts and legal norms of the public domain [4].

Conceptual Foundations of Digital Identity

The starting point for this discussion is the concept of a Digital Identity System (DIS). A DIS is a specific type of digital identity technology used to establish, authenticate, or verify an individual's identity in online contexts. These systems offer distinct data practices and governance arrangements that can critically affect privacy, access, and state capacity outcomes [4]. A common form of Digital Identity is a national identification scheme that assigns a digital identity and interconnected datasets to individuals at birth, often maintained through a mandatory or de-facto registration process [1]. Such systems create a national registry for the allocation of digital identities and, as a by-product, facilitate the creation of extensive datasets in the form of digital government databases [2]. Mandatory digital identity systems enable administrative authorities to create comprehensive datasets that can be used to monitor a broad range of public and private activities with minimal effort or cost [3]. The implications of DIS technology are far-reaching, spanning from potential surveillance abuses to restrictions on access to essential services, such as banking, education, health care, and financial aid programs [1]. The technology of modern state-derived Digital Identity has enabled administrative systems to expand their scope, scale, and reach over populations at an unprecedented rate [2].

Definitions and Scope

Digital ID systems have gained significant traction as countries strive to formalize citizens' identities, aligning their digital identification with pre-existing physical systems [1]. While countries such as India and Estonia pursue ambitious digital ID objectives, myriad challenges, including high-profile data breaches, have also emerged. To navigate these complexities, Digital Identity Systems, privacy, access, and state capacity outcomes define a Digital Identity System as an information technology-based solution that holds state-issued documents and other identity attributes [2]. Prior to the birth of the Internet, the central question of identity for national governments focused on formalizing the self's identity [3]. Digital Identity Systems aim to expand citizens' access to digital services. Privacy, access, and state capacity outcomes are closely intertwined, each impacting the others, yet these interrelations are frequently overlooked in the contemporary literature [3]. This framework allows for a systematic analysis of governmental document retention policies alongside a digital ID deployment evaluation framework. Prior to the COVID-19 pandemic, privacy, access, and capacity considerations rarely featured in debates surrounding digital ID systems. Global responses to the COVID-19 crisis, however, underscored the importance of public health service delivery, driving scholars and practitioners alike to develop solutions to enhance service delivery to marginalized populations, tackle misinformation, and fight systemic fraud [4]. Despite the immediacy of these concerns, privacy and data protection remain essential components of public service delivery [5]. The work focuses on the interplay between privacy, access, and state capacity outcomes in relation to Digital Identity Systems. Data practices are understood as the gathering, retention, processing, and dissemination of information [6].

NIJEP Publications

Governance encompasses the policy instruments, regulatory frameworks, and implementation modalities that authorities employ to achieve specified public goals [7]. Such practices can yield unanticipated consequences; for instance, reduced privacy protections may lead authorities to store digital identity credentials for extended periods, thus incurring associated risks such as data leaks, the expansion of databases, and legal ambiguities regarding digital certification [3].

Key Dimensions: Privacy, Accessibility, and State Capacity

Every digital identity system (digital ID) involves the collection, retention, and governance of sensitive personal data [2]. Systems therefore vary considerably in their governance and the privacy-related dilemmas they generate [1]. A comprehensive framework must distinguish between four privacy aspects: data minimization addresses the scale of data collected; consent governs the terms under which individuals agree to share data; control involves the extent to which individuals are empowered to determine data use; and autonomy pertains to the emergence of new dependencies that curtail individual agency [3]. Related concepts, such as civil liberties and exposure to surveillance, overlay this distinction and directly affect perceptions of system privacy [4]. Privacy dilemmas arise because the data practices required for effective identity governance often conflict with these four dimensions [5]. Higher levels of data minimization, consent, control, and autonomy are linked to lower state capacity [5]. Digital ID systems therefore generate different privacy–capacity trade-offs, which in turn interact with state capacity, programming, and the regulation of the digital economy to produce volatile outcomes across diverse political contexts [6].

Privacy Implications of Digital ID Systems

The growing trend in digital services like finance, healthcare, and education creates a pressing need for identification. Digital ID services are being introduced in many countries to improve remote verification, following advances in sociology and computer science that have shaped theoretical understanding of identity and its representation [3]. Different definitions of identity draw contrasting boundaries between the essence of identity and the social constructs that shape it [4]. The data contained in digital ID systems can be theorized either as data about identity or as data that constitutes identity. The modalities of representation in digital environments remain one of the enduring concerns of digital sociology [5]. Digital IDs reflect efforts to both control the democratization of technological access and transition between state control of technologies and regulation of those technologies. A precautionary approach is called for to navigate the governance dilemma created by digital IDs [6].

Data Collection, Storage, and Governance

All identity systems rely on data practices, which encompass the collection, storage, dissemination, and retention of user data [6]. Two broad categories emerge: those that store the data centrally and those that do not [2, 7]. Governance refers to the regime that determines how data practices are implemented [7]. The notion of an ID system extends beyond technology to encompass components such as management structures and legal frameworks. An administrative system that facilitates service delivery to the population constitutes a component of state capacity [8].

Surveillance Risk and Civil Liberties

Surveillance has evolved into a multifaceted phenomenon driven by the pursuit of diverse activities that can lead to gains in power, authority, or financial profit [6]. Emergent surveillance frameworks increasingly hinge on understanding the adoption and incorporation of new technologies such as those employed in digital identity management [7]. The advent of new and powerful technologies, combined with digital networks that enable the collection, transmission, processing, archiving, and synthesis of data at unprecedented rates, has accelerated the transition from one-off volumetric big data to pervasive surveillance as a service [8]. Consequently, the discourse has shifted from “digital identity” as a locus of access to digital services to “digital identity” as a nexus of surveillance, a reconfiguration that prompts closer examination of civil liberties and privacy issues. The proliferation of these digital network technologies fosters persistent, collaborative, and opportunistic surveillance, with the underlying trend toward a blend of physical bioprofiling and online digital profiling remaining intact [8]. Biometric technologies, which transgress the boundary of cyberspace by linking the digital and the corporeal, are expected to play a pivotal role [8]. Public authorities conceal vast biographics and biometric datasets assiduously gathered over long periods, thereby preempting feedback loops. With anthropometric and biodata capable of encoding an individual’s biohistorical narrative, state authorities and businesses have a particular stake in surveillance regimes [6]. Trust in government as an institution often correlates with perceptions of safety and security. An emerging trend involves the enhancement of digital surveillance penetration accompanied by advances in smart artificial intelligence, biometrics, and big data analytics [7]. Governments consider who collects what data, from whom, when, where, and how to draw inferences on behaviours, attitudes, feelings, and opinions, with security as a common underlying concern [8]. The hybridization of grand, mass, or extreme surveillance with indirect, ubiquitous, or espionage surveillance enables a geometry of power that influence the choices available to individuals [9]. Ultimately, data do not merely provide a passive infinite trail of evidence; both data and their visualization remain part and parcel of

NIJEP Publications

surveillance activism. Despite the sophistication of modernity, surveillance remains a social activity rather than some deterministic, technology-based, futuristic programme [10].

Consent, Control, and User Empowerment

Digital Identity Systems enable individuals to establish secure online accounts using local names, passwords, or biometrics; governments can verify that individuals are who they claim to be [6]. Such systems also permit individuals to control access to personal data linked to those accounts [7]. Data collected during verification and access control is expected to support policy decisions on civil liberties, inequality, and investments in infrastructure and other durable goods [8]. Many Digital Identity Systems grant users limited control of personal data. Individuals often receive no training on how to safeguard their privacy or even how to use the systems; experience with other Digital Identity ecosystems does not build confidence or competence. As a result, adoption often remains low among vulnerable populations at risk of social and economic marginalization [9]. Governments classifying Digital Identity Systems as high-risk have sought to enable users to determine when, how much, and with whom personal information is shared [10]. To address such concerns, the Section proposes a comprehensive approach to safeguarding consent and data access control [11]. The advantages of concurrent access to separate datasets for anonymized analysis are highlighted, along with specific social programs for which such access is critical yet sensitive [12].

Access to Identity and Inclusive Design

Nonetheless, even when identity and formal rights are guaranteed, individuals may still face barriers to access. Barriers such as low levels of digital literacy, lack of access to the internet or devices, and poorly designed platforms, applications, and processes can prevent individuals from access and limit the effectiveness of services- and state-capacity gains [5]. Moreover, the presence or absence of these barriers can directly influence the capacity to access services by groups in the population already engaged in or digitally excluded. Attention to these different forms facilitates the second substantive axis of the framework on access in relation to Digital Identity Systems [6]. Framed this way, three main questions can be asked to guide evaluation: [1] To what extent do people at different levels of digital literacy face barriers to access delivered services? [2] To what extent do people with limited access to the internet and devices face barriers to access delivered services? [3] To what extent are systems designed so that all citizens with a documented identity have access to the range of delivered services through digital channels that they could access through non-digital channels? [4]

Marginalized Populations and Digital Exclusion

Digital exclusion defines the challenges that some groups face in accessing and effectively using digital technology [9]. Marginalized communities, people with disabilities, low-income families, members of minority ethnic groups, and the elderly encounter obstacles when interfacing with conventional services [10]. Technological and societal barriers impede such populations in several ways: lack of infrastructure to connect devices, inability to pay for devices or connectivity, barriers to access, low digital literacy, and stigma associated with requests for assistance during service delivery [11]. Segregation and discrimination linked to poverty, citizenship status, education, social networks, and locations, as well as divergent adaptation rates to common technologies, exacerbate exclusion [12]. Consequently, the inclusive design of digital identity (ID) systems remains vital. Such systems should actively consider the abilities, language, cultural interpretation, and local context of all potential users when selecting and combining enabling technologies [13].

Interoperability and Portability

Interoperability and portability are critical aspects of identity management systems [1]. A variety of frameworks and standards have been developed to meet requirements for privacy, security, usability, and trustworthiness in these systems. However, significant challenges remain, including fundamental usability and security flaws, inherent risks associated with specific protocols, and privacy preservation in federated systems [2]. The identity metasystem initiative represents ongoing efforts to deliver privacy-compliant solutions [3]. Fundamental issues such as trust requirements, global identity management, and the establishment of interoperability standards across sectors and platforms are essential for effective identity management although [4]. For a Digital Identity System to enhance space for individual freedom and impact positively the day-to-day lives of users, interoperability, portability, and cross-border usability are required [5]. Such capabilities lower the hurdles entailed in the dissemination of the Drive Instruction, are, when implemented without the enforcement of proliferation provisions or restrictions in their own right, more easily accepted by multiple stakeholders when an identity ecosystem based on the provision of either a verifiable or a queryable credential permitting services to ascertain the user's identity is already deployed in the country, and permit potential access to economies of scale in the supply of the identity system's technical architecture, drawing in turn from the widespread availability of solutions for software provisioning in such markets [6].

Social Equity and Friction in Service Delivery

An efficiently functioning public administration, capable of providing services to its citizens and conducting regular national operations, depends on a nation's identification system [11, 5]. Identifying the identities of users effectively is not an easy task [7]. An evolution of more universal systems occurs when a digital identity system is able to cover a wider range of aspects such as private, health, commercial, educational and financial aspects. An extensive digital identification system can lead to an increased concentration on economic activities and enable service provision all around the world [8].

State Capacity Outcomes Linked To Digital Ids

Digital Identity Systems are often perceived as tools to promote service delivery and access to government welfare programs [4]. However, they may also 5 facilitate the introduction of ID systems; 6 increase transparency of fiscal transactions; and build confidence in civil society's willingness to access services and fiscal resources from government[5]. Digital identity systems connected to data provided directly by citizens and government agencies, with citizen control over data access and provision, increase civil society engagement with government and thus promote State Capacity outcomes such as Fiscal Extractive Capacity and Government Accountability [6]. State Capacity outcomes are linked to the perception that parts of a modern State must be legitimized through a Digital ID connected to services, transactions, or ID provision. Civil society engagement with government encourages Fiscal Extractive Capacity, measured by the percentage of Gross Domestic Product (GDP) collected in taxes, and Accountability, measured through the Freedom House rating[7, 8].

Administrative Efficiency and Service Fusion

The establishment of digital identity systems is fundamentally altering the relationship between service provision and administrative efficiency [5]. Prior to the advent of these systems the two concepts were largely viewed as separate and distinct. Digital systems facilitating remote access to services have allowed for their fusion into a single technical and policy domain [6]. Digital identity systems can improve service administration in two main ways. First, they enable remote provisioning of services, often replacing the need for in-person registration, verification, and authentication. This shift can greatly compress the time and cost typically spent on acquiring services in person [7]. Second, the administrative functions now enabled by digital identities open new avenues for preventing fraud in service delivery [8]. By verifying identity during the provisioning stage, agencies can dramatically lower the probability that a fictitious or stolen identity will successfully acquire a service [9]. Service-delivery processes that remain strictly in-person are much harder to monitor or control for such risks. Administrative efficiency gains become particularly relevant in situations where provision of service is legally mandated, but take-up rates and user awareness remain surprisingly low [1].

Fraud Prevention, Verification, and Governance

Digital identity systems are promoted as a means for governments to deliver services more efficiently, facilitate economic growth, and combat fraud [5]. This section maps the multifaceted interaction between fraud prevention, verification, and governance. Effective digital ID systems are anticipated to enable accurate verification of individuals while minimizing service-induced exposure [6]. Well-designed systems help governments detect flouting of regulations, mitigate systemic governance failure, and prevent inefficient allocation of resources [12]. Counter intuitively, however, augmenting verification can increase operational complexity and grievances, potentially exacerbating the very governance failures digital IDs seek to alleviate [13]. For digital ID systems to strengthen, rather than undermine, the social contract, they must be meticulously designed and implemented [14]. Governments worldwide emphasize fraud prevention and verification as major drivers for establishing digital identity systems [14]. Strengthening capacity to distinguish between legitimate and fraudulent individuals is seen as a means to increase state legitimacy [15]. Many countries view the emergence of synthetic identities fraudulent cases in which individuals are registered, obtain social goods, and often succeed in accessing digital financial services secured by these identities as an urgent challenge [16]. To address this problem, governments have begun implementing digital ID systems. From a broader perspective, efforts to curb fraud and verify clients are intertwined with the concept of governance [12]. Countries that control and sanction illicit market activities, even in informal economies, are considered more accountable and legitimate. Improving this capacity, therefore, is often regarded as an avenue to bolster the social contract [11].

Accountability, Auditability, and Governance Challenges

With a growing emphasis on digital identity systems in specialized fora, the question of how to ensure such systems are accountable, auditable, and governed is emerging as a central concern [5]. Despite the fast-paced headline-generation nature of many identity news stories, credible discourse typically concerns how to guarantee especially in terms of cross-border or intergovernmental systems continued and continual oversight, the possibility of third-party independent audit against stipulated governance frameworks, and accessible redress processes when commitments are visibly breached [6]. Accountability regimes concern state capacity, but also figure prominently

NIJEP Publications

in own access and privacy considerations [7]. Privacy implications arise primarily through digital ID governance, not the mere existence of digital ID or the technical structures underlying it [2].

Comparative Perspectives and Case Studies

The universally virtually acknowledged concept of identity is complex. For governance, it has primarily included five aspects: the definition of who a person is, the attributes associated with whom they are, what a person can do, the history of the actions performed, and the physical undertaking needed for action to budge the identity [6]. The definitive aspects of identity will receive more attention, as policy processes inevitably concerns the definition of a person and attributes allowing activities [7]. Governments issue identity documents like birth certificates, national ID cards, marriage certificates, and passports [8]. In every society, individuals possess “formal” official and “informal” unofficial identities [9, 10]. Various documents improve the stature and access of individuals to opportunities [11]. Technological advancement leads to the establishment of systems to unify identity management within government, economy, and society, both between governments and institutions and among institutions or agencies. Digital ID systems help states enhance their governance capacities, maintain national physical and economic security, and provide services like social security, transaction permit, and control of vaccine supply and appropriate fare levels [12, 13].

Regional Implementations and Policy Variants

This section synthesizes the core argument of the work and describes regional variations in Digital Identity System implementation [7]. Digital Identity Systems (DIDS) process citizens’ identity attributes to enable safety verification across online transactions [8]. Privacy, access, and state capacity dimensions shape the governance of these systems and frame policy choice: limiting exposure in design promotes privacy; prioritising transformational access encourages use among service-deprived groups; placing emphasis on efficiency-building activities supports service delivery on a wider scale. Over 30 states in Africa, Asia, Latin America, and Europe pursue DIDS [9]. Four implementation variants emerge, differentiated by legal framework unambiguous, ambiguous, or contested enactment and governance structure open, closed, or hybrid model [10]. These configurations modify how privacy, access, and capacity interact and determine where each capability sits along the spectrum from enabling to obstructive. Policy variants exemplified through country cases yield generalisable lessons on design choices influencing outcome effectiveness [11].

Lessons from Successful and Problematic Deployments

Digital identity (ID) systems differ considerably in design and implementation, reflecting diverse political and social contexts [4]. Such systems are substantively defined as technology, legislation, and governance arrangements facilitating digitally authenticated identity attribute presentation or access [5]. By mapping the characteristics of deployed systems across regions and drawing lessons from these experiences, governments may better anticipate potential challenges, realistically assess their systems, and refine policies that align with national priorities. Some cross-regional insights emerge from a comparative review of the design and implementation of digital ID systems across various jurisdictions [10]. The COVID-19 pandemic has prompted governments worldwide to digitize public services and promote digital identity schemes [11]. Crisis response experiences offer insights into the enduring potential of tools acquired for pandemic management. Taking a broader view, an expert investigation of systems already in place identifies critical design aspects to facilitate planned, effective, and inclusive delivery [12].

Methodological Considerations for Evaluating Outcomes

Digital Identity Systems (DIS) promise improvements in state capacity, citizen access, and privacy, distinct goals that risk conflicting if pursued independently [4]. A theoretically informed analytical framework connects these dimensions, generating a refined model of DIS outcomes and guiding the empirical examination of privacy, access, and capacity indicators in 89 countries [5]. Identity systems tend to enhance access and capacity while threatening privacy; governance choices determine the impacts [6]. Regional analyses of African, Asian, and Latin American policy variants examine how different legal, institutional, and technical configurations mediate DIS effects [7]. These investigations highlight crucial trade-offs and interaction dynamics, offering actionable insights for policymakers [8].

Metrics for Privacy, Access, and Capacity

Digital Identity Systems: Privacy, Access, and State Capacity Outcomes. France, Ghana, and India all maintain Digital Identity Systems that interface with national populations through the provision of data packets included in transactional exchanges [6]. Each of these systems provides different levels of oversight on the conditions under which data packets are made available and on the extent to which the frictionless completion of transactions through Digital Identity Systems can be enabled without explicit returns of data packets to the Data Resource Manager or other development partners [7]. To pursue the connections between a Digital Identity System’s design and the privacy, access, and state-capacity outcomes that emerge from the associated balance of these three dimensions, an analytical framework is constructed that embraces these independent dimensions of effect; formalizes the anticipated

NIJEP Publications

interdependencies that underpin a concerted action orientation toward each of the three observations; and articulates corresponding Metrics for Privacy, Access, and Capacity [8]. Combinations of these Metrics already exist and provide a foundation for exploring this proposal within these particular systems [9, 10].

Data Sources and Research Design

Digital identity systems now permeate many aspects of public life and increasingly mediate the safeguarding of access to public services [5]. More defined as systems that meet at least three conditions, separate digital identities for proof of identity and eligibility; registration of self-reported information about identity and eligibility; and operational data practices related to the collection, flow, storage, sharing, usage, and deletion of such data, these systems rely on governmental issuance of a digital identity and the creation of shared, formally-managed databases [6]. Within this framework a set of three state capacity outcomes is defined, comprised of administrative efficiency, fraud prevention, and governance accountability [1]. Identifying and characterizing broad patterns of cross-national arrangements across these dimensions provides the foundation for an analysis of access, privacy, and capacity effects across the first group of countries [4]. Digital identity systems governing three country cases Venezuela, Colombia, and Mexico are then sketched, framed in conjunction with formal data governance arrangements, and related to both specific and general patterns across the remaining countries [7]. Addressing data obligations and ethical practices across the second group of countries calls for examination of sixteen varied arrangements employed in conjunction with digital identity systems [10].

Ethical Considerations in Evaluation

Digital Identity Systems (DISs) raise significant ethical questions. A key concern lies in how DISs affect citizens' control over their personal information [6]. National-level DISs usually entail the collection of biometric or personally identifiable information at large scale, often linked to a broader governmental plan for digitalisation and e-governance. Consequently, the information can be persistently associated with an individual's identity and shared among multiple services [7]. Despite the collection of personal information, many governments still provide limited technical means for citizens to control their data. In general, citizens retain minimal control over the number of data points collected, how information is used, and with whom it is shared [8,9]. As DISs often determine access to vital services such as health care, social welfare, financial services, and education, this lack of control may be especially concerning [10, 11]. DISs that implement information sharing without adequately addressing citizens' capacity for oversight could raise substantial ethical issues related to agency and power imbalance between citizens and the government [12, 13]. These questions on control and autonomy must be examined within the broader context of the political and administrative goals of DISs [14]. Many states view DISs as crucial enablers for developing a digitally enabled government. Such a transition entails a clear shift in the infrastructure and layers of services provided for citizens, with the desired outcome of enhanced service accessibility, efficiency, and effectiveness [15]. The degree to which prioritising citizens' agency at the early stages of their digital transformation remains a common consideration relevant to DISs warrants further exploration [15].

Policy Implications and Governance Recommendations

The comparative analysis suggests five critical governance clusters for the successful design and implementation of Digital Identity Systems [4]. Policymakers consequently face the challenge of optimizing privacy protections while meeting the legitimate administrative imperatives of modern, responsible statehood empowered by access to digital ID space [1]. The challenge becomes even sharper given the contrasting socio-economic, political, and cultural characteristics of the different blocks and differing strategic interests shaping the incorporation of Digital Identity Systems into social and economic policy domains [3]. The Singaporean model may be attractive for its cutting-edge privacy-protective design and its unobtrusive integration with data-hungry Smart nations initiatives fully embedded into the urban, as well as bureaucratic environment [4]. The model also permits a potentially wide-ranging application of the Digital Identification System to mobile services beyond the Ministry of Finance's original concern with tax compliance [2]. Conversely, the Indian approach remains highly relevant because its Digital Identification System addresses from the outset a pressing development challenge arising not just from the scale, but also from the depth of exclusion in many Emerging markets and Developing countries, alongside the shunning of the physical Identity verification undertaken by the substantial number of E/M customers who may remain dependent on Knowledge-Based Authentication (KBA) mechanisms [3].

Balancing Privacy with Administrative Needs

Digital Identity Systems (DIS) offer a wide range of administrative applications, from flexible access to public and private services to enhanced means for protecting personal data [6]. Three systematic patterns of influence emerge from a comparative analysis of national deployments of DIS in the Global South. The first pattern traces the interplay between privacy and access. Initially prioritizing security considerations related to potential misuse, DIS widely implementing robust privacy safeguards subsequently turned to access [7]. The second pattern concerns access and state capacity. Considered a precondition for state capacity enhancement, access subsequently assumed a

NIJEP Publications

more nuanced role. The third pattern relates privacy and capacity [8]. Initially appearing to operate in opposite directions, subsequent developments indicated an interactive relationship. Because high privacy legislation, governance, and compliance levels are time-consuming to acquire, pursuit of capacity and oversight also a privacy consideration frequently occupied an intermediate position [9]. In terms of privacy, national approaches differ on data minimization, consent, control, and autonomy. In many instances, data minimization is a constitutional or legislative requirement governing the collection and processing of personal data. Regulatory frameworks also specify conditions enabling data collection [10]. Some Digital Identity Systems (DIS) loosen restrictions, allowing longer storage with an obligation to anonymize. Extended periods can be justified for statistical research, historical archives, and security purposes, with clauses mandating destruction after a specified duration [11]. Other cases emphasize a limited span, with the number of eligible justifications kept to a minimum without extending duration. Control predominantly relates to user involvement in the administration of the identity system, encompassing influence over setup, monitoring of operations, and remedial actions [12]. Autonomy is the personal right to determine one's own path in life and to gain insight into the suite of items existing along that path [1]. Where personal data storage has been completed, some systems permit users to control their own access to the data and to govern who sees what [2].

Ensuring Inclusive Access and Digital Literacy

Digital inclusion refers to the fundamental right of individuals and communities to access and effectively utilize information and communication technology for meaningful participation in societal, economic, and political spheres [11]. Digital Identity Systems (DIS) represents a pivotal dimension of the digital transformation agenda and plays a crucial role in realizing the digital inclusion agenda [12]. Establishing a DIS policy that guarantees inclusive access to Digital ID (DID) systems, along with a minimum level of digital literacy, is vital to foster a safe and secure digital citizenry and promote digital economy initiatives [13]. Citizens can only access and make meaningful use of state and private services effectively when the required technical and technological infrastructure encompassing devices, networks, applications, and platforms aligns with their existing level of financial and digital literacy [12]. The internationally recognized "GAP" framework categorizes the access to technology required for public service delivery into dimensions such as availability, affordability, accessibility, capacity, and interoperability [13]. Building on these national and international standards, the following minimum DID access indicator is proposed: percentage of individuals who possess a Digital ID (DID) and have access to a mobile device or a personal computer connected to the Internet, combined with a minimum acceptable standard of digital skills determined by local authorities [14]. This indicator serves as a relevant proxy measure for evaluating the accessibility of Digital Identity Systems (DIS) and can contribute to policy and decision-making regarding Digital Identity System (DIS) inclusivity [5]. Gender, socio-economic status, age, geographic location, and disability comprise commonly identified barriers to the level of digital literacy that female citizens, poor households, the elderly, rural inhabitants, and citizens with disabilities can achieve. Information on such disparities, determining the levels of digital literacy they can achieve, forms a vital part of evaluating public service delivery accessibility [15]. A Digital Literacy Technical Indicator would therefore be an appropriate additional measure for this purpose. Digital Literacy Technical Indicators defined by relevant authorities that provide a clear policy that is an appropriate additional measure for this purpose [16]. Assessing the extent of Digital ID access consequently serves as a crucial prerequisite for evaluating full access to Disaster Risk Management (DRM) information and services. Those without a Digital ID cannot access interactive government platforms even if equipped with the necessary devices and disseminating IDM services exclusively through these channels is a foreordained disadvantage [15]. The European Commission defines that "every person aged 12 or above" must be able to use a Digital ID, and all policy actions consequently center on this target. Accordingly, these indicators digital platforms and Disaster Risk Management have only partially been examined [16]. Since the onset of the COVID-19 pandemic, public services have solely been provided through online channels in numerous economies, rendering the Digital ID constraint exceedingly pertinent; nationwide assessments of open government data provision and related indicators have remained untouched in these contexts [14].

Enhancing Transparency, Accountability, and Redress Mechanisms

Governments, companies, and international organizations routinely collect, store, and control increasing amounts of personal data. Only a portion of this information engages directly with an individual's identity [13]. Digital Identity Systems are a subset of 'digital ID' systems that rigorously manage information about people's identities. Digital Identity Systems manage data relating to personal identity, driving a subset of digital public service provision [14]. They establish two-way connections between citizens and governments and between citizens and businesses. Governments manage these systems to bolster the provision of essential services and reduce the digital identity gap between the richer and poorer segments of the population [5]. Regulatory barriers at the point of public and private service delivery, however, still need to be addressed [7]. Digital ID currently does not drive the ultimate evolution toward digital convocation that a full transition from identity to identification requires [5].

Future Directions and Emerging Trends

The evolution of identity systems is an expected trend in the ongoing digital transformation [2]. The emergence of Digital Identity Systems (DIS) that protects user identity by means of cryptography, decentralization, and other forms of technology is anticipated [6]. The use of decentralization of identity attributes is expected to solve current issues related to unwanted usage of identity data by id systems [1].

Federated and Privacy-Preserving Architectures

The multinational United Nations (UN) Economic Commission for Europe (ECE) defines digital identity management systems as those enabling “the identification of individuals, their attributes (data) and authentication of identity in an online environment” [14]. Such digital identity management systems commonly comprise processes and technologies that perform three major functions: identity creation and capture; identity verification and authentication; and attributes management concerning such identity/identities [3]. Digital identity systems often employ federated architectures, where a user authenticates to a local service provider and obtains an assertion of identity accessible to other service providers, without requiring a national personal identity or informational identity card [15]. Even national systems that adopt a centralized architecture can implement a non-disclosing or federatable solution, storing only the public key while replication of the private key exists solely within the personal device [16]. Such federated architectures utilize privacy-preserving technologies such as zero-knowledge proofs, allowing both verification of age or attributes without data disclosure, and re-encryption, enabling credential transformation for different service provider requirements [16].

International interoperability and portability

The European eIDAS Regulation establishes the legal framework for cross-border recognition of electronic identification across the European Union [14]. This effort is complemented by the bilateral Mutual Recognition of Digital Identity agreement between the United Kingdom and the Republic of Estonia, which aims to enable seamless online identity verification between the nations. Despite being designed to facilitate interoperability, the eIDAS Regulation falls short of establishing a universal framework for federated identity management that can readily accommodate new services or guarantee compliance with national regulations [15]. For global interoperability and portability, initiatives such as the Identity Metasystem seek to define a set of standards and best practices for identity management that can be adopted internationally [16]. The aim is to provide end users with assurances about appropriate privacy, security, usability, and user-centricity concerning their digital identities, irrespective of the specific identity management implementations in use [1].

Adaptation to Evolving State-Society Relations

Digital forms of identification policy support state adaptation to evolving power relations with society. As democratic accountability in Western democracies erodes and electoral outcomes are contested in authoritarian states, technologies favoring state control are gaining popularity [15]. Digital identity initiatives in Africa offer insights for state-society balance adaptation [16]. Countries such as Kenya, Nigeria, and Tanzania are implementing digital identity initiatives for purposes including disbursement of social services and universal access to essential services [15]. The rapid implementation of these large-scale and potentially far-reaching identity systems poses multiple questions concerning governance, privacy, digital exclusion, and state capability [6].

CONCLUSION

Digital Identity Systems represent a significant development in modern governance, offering opportunities to strengthen state capacity, improve public service delivery, and expand citizens' access to essential resources. However, their effectiveness depends not only on technological advancement but also on the quality of governance frameworks, institutional arrangements, and protections established around personal data. The analysis reveals that DIS operates within a complex relationship between privacy, access, and state capacity, where improvements in one dimension may create tensions with another. While digital identity infrastructures can enhance administrative efficiency, reduce fraud, and promote accountability, poorly designed systems may deepen social exclusion, enable surveillance, and undermine citizens' control over their personal information. The future success of Digital Identity Systems requires a citizen-centred approach that prioritizes inclusivity, transparency, and accountability. Governments must ensure that digital identity initiatives are supported by strong privacy regulations, meaningful consent mechanisms, effective oversight institutions, and accessible grievance-redress systems. Equally important is addressing digital inequalities by improving connectivity, digital literacy, affordability, and usability for marginalized populations, including rural communities, low-income groups, older persons, and persons with disabilities. Privacy-preserving technologies, interoperable frameworks, and user-controlled identity models provide promising pathways for developing more secure and empowering systems. Ultimately, Digital Identity Systems should be understood as instruments of social transformation rather than merely administrative technologies. Their long-term legitimacy will depend on their ability to strengthen the social contract by enabling inclusive participation, protecting fundamental rights, and building trust between citizens and governments. A balanced

NIJEP Publications

approach that combines technological innovation with ethical governance is essential to ensure that digital identity systems contribute to equitable development, democratic accountability, and sustainable state capacity.

REFERENCES

1. Alpár G, Hoepman JH, Siljee J. *The Identity Crisis: Security, Privacy and Usability Issues in Identity Management*. Nijmegen: Radboud University Nijmegen; 2011.
2. Hardjono T. A federated authorization framework for distributed personal data and digital identity. *IEEE Commun Stand Mag*. 2019;3(4):56–62.
3. McLaughlin M, Briscoe G, Malone P. Digital identity in the absence of authorities: A new socio-technical approach. In: *Proceedings of the International Conference on Social Computing*. Minneapolis (MN): IEEE; 2010. p. 809–814.
4. Chaudron S, Eichinger H. *Eagle-Eye on Identities in the Digital World*. Luxembourg: Publications Office of the European Union; 2017.
5. Spiliotopoulos T, Sheikh TA, Gottardello D, Dover R. *Onboarding Citizens to Digital Identity Systems*. Luxembourg: Publications Office of the European Union; 2023.
6. Hum M. Biometric ID cybersurveillance. *Surveillance Soc*. 2013;11(4):426–440.
7. Manohar A, Briggs J. Identity management in the age of Blockchain 3.0. In: *Proceedings of the International Conference on Blockchain Technology and Applications*. New York (NY): ACM; 2018. p. 45–52.
8. García Sanz RM. Rethinking privacy to define surveillance. *J Inf Commun Ethics Soc*. 2014;12(4):257–273.
9. Sannon S, Forte A. Privacy research with marginalized groups: What we know, what's needed, and what's next. *Proc ACM Hum Comput Interact*. 2022;6(CSCW2):1–33.
10. Dosono B. Patron privacy: A luxury concern for marginalized internet users. *Proc Assoc Inf Sci Technol*. 2019;56(1):754–756.
11. Heinsch M, Tickner C, Kay-Lambkin F. Placing equity at the heart of eHealth implementation: A qualitative pilot study. *Int J Equity Health*. 2022;21(1):1–12.
12. Whitley EA. Trusted digital identity provision: GOV.UK Verify's federated approach. *Comput Law Secur Rev*. 2018;34(4):897–914.
13. Coles-Kemp L, Ashenden D, O'Hara K. Why should I? Cybersecurity, the security of the state and the insecurity of the citizen. *Politics Gov*. 2018;6(2):77–98.
14. Sun N, Esom K, Dhaliwal M, Amon JJ. Human rights and digital health technologies. *Health Hum Rights*. 2020;22(2):21–32.
15. Gautam A. *Usable, Acceptable, Appropriable: Towards Practicable Privacy* [doctoral dissertation]. London: University College London; 2020.
16. Zwattendorfer B, Slamanig D. The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality. In: *Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES)*. Salzburg: ACM; 2016. p. 629–638.

CITE AS: Kabiga Chelule Kwemai (2026). Digital Identity Systems: Privacy, Access, and State Capacity Outcomes. NEWPORT INTERNATIONAL JOURNAL OF ENGINEERING AND PHYSICAL SCIENCES,6(1): 1-10.
<https://doi.org/10.59298/NIJEP/2026/611000>