©NIJCRHSS
Publications

Open Access
Print ISSN: 2992-6106
Online ISSN: 2992-5789

NEWPORT INTERNATIONAL JOURNAL OF CURRENT RESEARCH IN HUMANITIES AND SOCIAL SCIENCES (NIJCRHSS)

Volume 6 Issue 1 Page 1-10, 2026

https://doi.org/10.59298/NIJCRHSS/2025/61.110000

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

Lubega Midlage

Humanities Education Kampala International University Uganda

Email lubega.midlage@kiu.ac.ug

ABSTRACT

Digital identity systems have emerged as a central component of modern governance as governments seek to improve service delivery, strengthen administrative efficiency, and enable secure digital interactions across public and private sectors. While these systems promise expanded access to services such as banking, social protection, education, and e-government, they also raise significant concerns related to privacy, inclusion, and state capacity. This paper examines digital identity systems through a conceptual framework built around three key dimensions: privacy, access, and state capacity outcomes. It analyzes how design choices such as data minimization, consent mechanisms, and verification technologies shape privacy protections and influence risks related to surveillance, profiling, and data misuse. The study also explores the challenges of ensuring equitable access, particularly for marginalized populations who may face barriers related to digital literacy, infrastructure limitations, language, and identity verification requirements. In addition, the analysis considers the potential of digital identity systems to strengthen state capacity by improving administrative efficiency, reducing fraud, enhancing transparency, and facilitating more effective service delivery. Evidence from national initiatives and cross-border identity systems highlights the trade-offs that policymakers must navigate between privacy protection, system utility, and governance efficiency. The paper concludes that successful digital identity systems require carefully balanced policy design supported by strong legal frameworks, inclusive access strategies, and transparent governance mechanisms. By integrating privacy safeguards, equitable access policies, and institutional accountability, digital identity systems can contribute to improved governance outcomes while protecting fundamental rights in increasingly digital societies.

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

INTRODUCTION

Digital identity systems frequently arise in the context of globalization and technological advancement. The need to manage access to an increasing number of services from banking to e-government has generated various forms of official and unofficial identification [1]. States respond to citizens' and residents' social and economic demands by establishing, maintaining, and distributing identity credentials, sometimes with the aid of the private sector. Analysts demand rigorous, evidence-based assessments to inform design and to optimize utility [1]. Digital identity systems significantly affect access to and inclusion in societal activities. A wide range of services, including education, skill development, employment, remuneration, legal rights, e-commerce, consultation, agriculture, social protection, and e-banking, depend on official identity verification [2]. Therefore, choices surrounding digital identity design and implementation impact marginalized populations with low access to national identification; public consideration of security, privacy, and access must extend to these groups, together with sensitive design around equity [3].

Open Access
Print ISSN: 2992-6106
Online ISSN: 2992-5789

Conceptual Framework

Digital identity systems are an emergent phenomenon that invites considerable empirical scrutiny. Pragmatism suggests that a flexible framework for analyzing policy questions might clarify matters for both scholars and institutions [1]. Privacy, access, and state capacity provide potential organizing themes. The privacy domain encompasses issues of collection, consent, surveillance, and redress [2]. Transparency, outreach, accessibility, and user control frame the access question. Governance, efficiency, fraud, and resilience inform state capacity considerations. Each shows considerable promise, yet none proves entirely adequate [2, 3]. Digital identity offers a partial solution to the "digital divide," the disparity between those with, and those without, access to the internet, as well as to rising demands for verification of electronic interactions via web-centric forms of identification [2]. Efforts to "bridge" such divides must acknowledge the existence of "cross-cutting" cleavages between specific identity-affected populations across high-, middle-, and low-. Within this constraint, existing identity regimes are examined alongside current technology on the evolving frontier of digital identity systems. State capacities attendant to governance, efficiency, verification, fraud, and resilience are also considered [3].

Privacy Implications of Digital Identity

Digital identity systems fundamentally alter the conditions under which private information is shared, hence generating privacy-related risks and consequences that differ markedly from those associated with traditional identity systems [2]. Specifically, privacy outcomes are defined, during their design and operation, by the extent to which systems champion data minimization, integrate reliable redress and appeal mechanisms, and strive to limit downstream risks of surveillance and profiling [3]. Data minimization, as stressed in the GDPR, is a principle that supports privacy preservation by limiting the potential for serious privacy violations. Such incidents are much more likely to occur if large amounts of data are collected, compared to cases where only a minimal dataset is made available. Although data minimization is often associated with auditing and data requests undertaken by state authorities, digital identity systems solicit information from populations in a manner that breaks new ground in terms of privacy implications [4]. Private information is shared with authorities in a much less discreet and one-sided manner than in most current identity systems. And the risks associated with reconciling private information held by various state authorities are much more serious than those associated with the current case of the identity card [3]. The invitation to GDPR-like protection thus evokes unintended consequences and trade-offs. Digital identity systems have the potential to enhance trust and minimize privacy risks only if they are accompanied by the establishment of legal frameworks and institutional mechanisms that adequately bolster the consent and auditing dimensions of privacy [2].

Data Minimization and Consent

Digital identity systems often require the collection of a comprehensive set of information, posing risks to privacy and security through unrestricted and unqualified access to personal details, even when unnecessary for service provision [1]. A governing principle for such systems must thus be to limit data disclosed in order to minimize exposure to harm. Upholding individual agency over personal information is similarly critical [2]. Users should remain in command of their data, consenting only to what and who they wish. Systems should therefore strive to render the collection and sharing of information more transparent, allowing individuals to grasp the implications of their choices and to exercise broader control [3]. Well-structured consent procedures, justifiable requests, and clear subsequent obligations enhance understanding and autonomy. Applicable to a wide array of contexts, these principles foster privacy, mitigate surveillance, and fortify governance [4]. They gain particular salience in regions where the integrity of the public sphere is compromised, enabling vulnerable populations who commonly labor under the gaze of the state to engage with official apparatuses without exposing themselves to further scrutiny [3].

Surveillance, Profiling, and Freedom

Digital identity systems put demographic and transactional data in the hands of governments and private companies for verification or authentication purposes, potentially enabling state and corporate surveillance of individuals [2]. Concerns about social control have arisen because identity information compiled over time can facilitate social profiling and, consequently, exacerbate marginalization and ostracism [4]. The risk of violation of civil liberties is aggravated in states with a history of repressing political dissent, and where a predominant worldview grants corps entrenched market power and an asymmetric ability to influence political choices. Sweeping statements about the coercive capacity of the state, the omnipresence of surveillance capitalism, or the results of imaginary thought experiments are unhelpful for intelligent policy design in these political-territorial truths. States with agency, capable of negotiating their interests, can be better served by identity systems that enhance capacity and governance [5]. A differential evaluation of identity systems with respect to privacy, access, and capacity outcomes guides policy advice towards design choices that enhance privacy without compromising the utility of identity systems and the efficiency of administration[3]. Identity systems are a powerful driver of datafication and an enabling environment for surveillance capitalism. The structured and machine-readable

Open Access
Print ISSN: 2992-6106
Online ISSN: 2992-5789

identity data can be combined with human action data in commercial transaction logs to build a complete data profile on individual behavior and preferences [2]. Specific privacy concerns arise from the data sets controlled by governments (Smith, 2020). In liberal democracies, historical experience with state surveillance raises concerns about the capacity of identity systems to facilitate political and corporate control over individuals and society. In societies with entrenched social inequality, elevated risk of state repression, and a pro-business orientation, the introduction of digital identity systems is perceived as a threat, particularly when a social credit-style scheme is accompanying implementation [1].

Trust, Rights, and Redress Mechanisms

Privacy risk increases when individuals cannot rely on trusted intermediaries. To address this, states need to underpin their digital identity systems with trusted rights and redress mechanisms [2]. Digital identity grants the state new powers, altering the social contract underlying citizenship. This reconfiguration must be transparent and subject to checks and balances to maintain a robust societal contract [5]. Citizens must retain their fundamental rights irrespective of their digital identity status. Privacy concerns persist, including how data is collected and who has access to it [1]. Personal and location data are perpetually sensitive and require rigorous protection. Strings of 1s and 0s are identical irrespective of content, so individuals and businesses must have assurance and recourse regarding data use [2]. Recent initiatives to establish trusted data management and sharing systems highlight these issues.

Access and Inclusion

Governments worldwide support the rollout of digital identity systems on the promise of greater access to services, goods, and benefits for citizens [8]. However, the requirements of those systems can themselves become barriers to access, particularly for vulnerable and marginalized groups, disadvantaging the very populations system designers seek to include. Poor usability, lack of outreach, unavailability of vernacular languages, and low levels of trust and digital literacy further limit inclusion [6]. To avoid unintentionally locking vulnerable populations out of access to entitlements and services, developers can maximize system participation if they pay close attention to target populations and to human-centered design and behavioral-engineering approaches. Several onboarding models can accommodate diverse user needs, including self-verification with anonymously issued credentials, system-assisted verification, and a non-verification "minimum viable identity" that enables services not requiring a full identity check [6]. Users forced to comply with nondigital identity-sharing requirements after getting a digital identity also retain the ability to self-select to remain nonpersonalizable by the system in all communications [6]. The rollout of digital identity systems worldwide is frequently accompanied by promises of improved access to services, goods, and benefits for citizens. Paradoxically, however, the very requirements of these digital identity systems can themselves become barriers to access. Vulnerable and marginalized populations already frequently lack the desired credentials and therefore remain disadvantaged when designers assume they do [5]. Accessibility further diminishes because the systems are not usable. Additionally, existing engagement often obscures target populations, limiting options to those unmet needs. Marginalized groups additionally suffer from poor user experience, the absence of service-related vernacular languages, and low levels of trust and digital literacy [7]. Therefore, digital identity systems risk withholding access to entitlements and services unless designers monitor barriers experienced by potential users throughout implementation efforts.

Digital Divide and Marginalized Populations

Accessible and inclusive digital identity systems are preconditions for achieving their intended benefits. Failure to address barriers such as those related to access obstacles, literacy, or usability may perpetuate or exacerbate social inequalities [4]. The design and roll-out of digital identity systems must therefore heed the needs of marginalized populations, many of whom are disproportionately affected by the lack of a formal identity. Member states must ensure that identity systems do not reinforce existing levels of exclusion associated with the digital divide [5].

A successful digital identity system provides equitable access to its services for all populations, irrespective of their social or geographical background or the level of resources of the places where they live [3]. Particular attention needs to be given to the most disadvantaged segments of society, which are often affected not simply by poverty, but also by other factors acting in conjunction with it (disability, gender, climate change, linguistic minorities, refugees and displaced persons, etc.)[5]. Specific attention should also be devoted to issues of protected characteristics and remote areas where a lack of infrastructure may hinder access to services offered through the digital identity system [4].

Accessibility, Usability, and Language Considerations

Digital identity systems have emerged as a crucial instrument to comprehensively tackle user authentication and identification [3]. Digital identity indicates the representation of an individual's online presence in the digital environment, which can be categorized into three types: national, organizational, and personal [7]. Consequently, digital identity systems are established as a unified hub for both public and private sector transactions. Within the digital identity paradigm, digital identities can be identified regardless of context, supporting meaningful and

Open Access
Print ISSN: 2992-6106
Online ISSN: 2992-5789

secure interactions [4]. However, the expansion of the digital identity framework has also raised serious concerns regarding the users' right to privacy. Therefore, it becomes imperative to analyze digital identity systems from the perspectives of privacy, accessibility, and state capacity [6].

Identity Verification Methods and Barriers to Access

Identity verification methods shape access to identity systems, especially among marginalized populations. Biometric checks are often employed, but they raise the stakes of failure, especially among disadvantaged users. Biometrics can enhance convenience, ease, and trust, yet can also hinder usage and support prejudice [9]. In particular, failure during verification can deter use without remedial actions [5]. Alternative methods, well communicated through appropriate channels, may be more appropriate or convenient for some users. Furthermore, identity systems may impose usability and policy burdens that act as barriers to access, such as account, device, or service fees, and location or jurisdiction limits. Such risks and barriers must be examined to facilitate equity and inclusion in system access [7]. To support unhindered access to identity systems, all eligible users should be able to complete verification and registration processes consistently across geographic locations, and using their preferred language, with minimal need for assistance, and without incurring charges [8]. The settings, information, support materials, and user interfaces of electronic remote registration and verification processes should be comprehensible, intuitive, consistent across channels, and responsive to patterns of activity among low-literacy or low-technology users [4]. For biometric verification, models trained on appropriately representative datasets and error-handling approaches that support access and continued use among all users should be employed [3].

State Capacity and Governance Outcomes

A well-designed digital identity system can improve state capacity by enabling more efficient administration, greater inter-institutional collaboration, and enhanced service delivery. Digital identity leads to lower fraud levels, increased security, and greater operational resilience [6]. Moreover, it fosters better monitoring, transparency, accountability, and citizen engagement. In advanced economies with automated taxation, indexing of services on income or wealth mitigates the risks of exclusion [8]. To address fraud in procurement, the Estonian government developed a digital, fully trackable online procurement system with e-bidding, a digital signature, secure smart cards, and a national digital identity system. These measures, combined with a risk-based post-control system and rules on conflicts of interest, have significantly reduced procurement fraud [9]. Digital identity, by enabling online and location-independent service provision over the Internet, can facilitate and reinforce the decoupling of service and physical locations. The Estonian e-Governance Academy reports that digital identity technologies such as electronic signatures, sealed documents, and timestamping have made online government services 40% easier to access since 2010[9]. By enhancing transparency and accountability, digital identity can limit discretion, corruption, and rent-seeking, as well as raise citizens' confidence in the state. Services such as real-time tracking of applications, online justifications for decisions and refusals, online payments, and digital auditing increase control over and confidence in public administration [7].

Administrative Efficiency and Service Delivery

The primary rationale for establishing a digital identity system is to improve the efficiency, accessibility, and quality of public services [6]. A well-designed digital identity can facilitate the verification of user identity for a broad range of public and private services, thereby reducing the cost of service delivery. For instance, e-KYC mechanisms allow financial institutions to remotely verify customer identity and complete the onboarding process without the need for physical documentation, thus lowering costs and enhancing the availability of financial services [6]. Similarly, existing residents can use their digital identity to obtain welfare benefits and bank accounts through a simple online process, while digital onboarding enables interoperability and more cost-effective account opening abroad [3]. However, the administrative efficiency associated with digital identity could come at the expense of less popular and less efficient services. Government infrastructure is often designed to minimize costs of delivery, rather than to ensure that the true demand for services is met [8]. Demand-driven approaches, which are more resource-intensive but better at reaching the poor, are recognised to be the right approach when budgets are tight, and the rich are able to access private alternatives [5]. The ability of a digital identity system to enhance cross-border movement of people would also facilitate the role of the private sector in providing identity services, such as e-KYC for online account opening, and supersede the need for government-issued cross-border identity assurances. Both aspects could result in a loss of welfare for vulnerable groups [3].

Fraud Reduction, Security, and Resilience

Fraud is a major issue for identity systems, and, as the literature on anti-money-laundering and anti-terrorism financing regulations suggests [3], includes systemic components intended to prevent fraud and subsequent incidents of unauthorized identity use. These characteristics will contribute to security and prevent crime. For governments, these components offer an opportunity for international cooperation against fraud and money laundering [3]. The persistence of identity fraud represents a considerable risk not only for government agencies

Open Access
Print ISSN: 2992-6106
Online ISSN: 2992-5789

employing strong authentication mechanisms, such as ePKI, but also for private-sector entities that issue identity documents (ID cards, passports, residence permits) without similarly rigorous processes[9]. If users cannot correct or even access their own data, they risk a major infringement on their life and personal development, weakening their relations with the state and society and making them more easily exploitable by criminals. In view of the massive resources devoted to infrastructure, research, and development, the large-scale deployment of smartphones in developed countries, and their increasing diffusion in developing countries, the main focus of future identity initiatives should be ease of implementation, integration into everyday life, and user convenience [8]. Indeed, the digital channel has made progress in allowing simple, fast, and cheap verification of identity attributes. Failure to put this opportunity to full use will lead to the same exclusion experienced by many of those who could not even afford a boiled egg at the time of the 2008 Beijing Olympics [8].

Institutional Transparency and Accountability

Inadequate institutional transparency and accountability are major obstacles to enhanced governance performance in numerous countries [3]. Digital ID systems ideally provide a convenient mechanism for citizens to obtain information about and lodge complaints against government agencies, thereby enhancing accountability. Digital ID reduces the extent of impersonation and simplifies data matching and tracing, both of which support fraud detection [5]. Therefore, when digital ID functions as intended, it fosters accountability of state institutions. Nevertheless, the literature on digital IDs' impact on these dimensions of governance remains relatively thin [6].

Accountability is central to any state's institutional development. Given the high degree of distrust and grievance that most citizens harbor for their governments, institutions, policies, and Politicians, citizens' participation in governance is often pessimistic. Such participation in the present context may take the form of complaints regarding public services delivered through the digital ID system and seeking redress. Digital ID reduces impersonation in the complaints process, thereby improving the transparency of the redress function [7]. The matching of complaints with transactions and records of public service delivery within the digital ID database enables instant verification of complaints and reduces the administrative workload and response time for redress [6].

Trade-offs and Policy Design

Trade-offs are a part of any policy design, and achieving desirable outcomes on one objective may hinder achievement of results on another [6]. Evidence, however, can help to inform decision-making. For example, balancing privacy with utility. All digital identity systems carry with them a risk of excessive and inappropriate collection of individuals' data, use without consent, or even the fundamental threat to individual freedom posed by omnipresent monitoring and profiling [5]. Yet, removing these risks altogether through principles, such as data minimization and personal consent, may create a system that is publicly useless, unable to deliver key services such as identity verification for purposes relating to anti-terrorism and anti-money-laundering activities, reducing the system's credibility among external stakeholders (such as financial institutions), and becoming difficult to justify to taxpayers. Ensuring equity alongside efficiency. Marginalized populations (including, to some extent, refugees and the homeless) are typically more difficult to reach, and their needs in terms of accessibility and usability are more pronounced and costly to accommodate [7]. However, when the costs of tailor-made adjustments are borne by others (such as the private sector) rather than the government, focus on efficiency or, rather, narrow, quantitative conceptions of efficiency will shift attention away from these citizens, hence aggravating existing inequalities [9]. Achieving positive governance or oversight outcomes also requires an adequate legal framework, and having a dedicated stakeholder in charge of the system with sufficient clout to energize, enforce, and keep everyone accountable can trigger positive outcomes for governance-related variables even in highly complex environments[8]. Consequently, trade-off analysis should also help identify which governance and legal arrangements are most likely to minimize the chances of negative outcomes in each dimension. Responsible policy design recognizes that there are no silver bullets; there are only bullets [10].

Balancing Privacy with Utility

A unique characteristic of digital identity systems is that the design choices and privacy outcomes are mutually dependent on the desired services, applications, and use cases [1]. For instance, a digital identity system only intended to support basic functions, such as confirming that a person has an official identity without specifying nationality, age, or unique identifiers, would require fewer data and therefore likely maintain a higher degree of privacy [3]. Conversely, a system with digital credentials permitting access to programs such as e-voting or digital currency is by its very nature less privacy-respecting, since functionality implies that the subjects of these credentials are publicly known [1]. Design deliberations must also account for how particulars of the system structures each of the privacy-related criteria enumerated above. For example, a system requiring active consent at the moment of every personal data access may achieve higher privacy scores than one relying on comprehensive prior consent. Yet, exact trade-offs remain heavily evolutionary and context-dependent, with only long-established norms and conventions beginning to solidify [10].

Open Access
Print ISSN: 2992-6106
Online ISSN: 2992-5789

Ensuring Equity alongside Efficiency

Efforts to enhance administrative efficiency, fraud reduction, and service delivery through the introduction of digital identity systems might unintentionally push some users outside the system [9]. Economies of scale can result from fewer errors, greater automation, and the shift from physical to online service delivery. More efficient systems can also deploy more administrative resources to serve remaining users [6]. Fraud reduction could enhance system resilience, but excessive focus on fraud reduction can impose costs on users. Marginalized populations incur greater system costs from strict identity verification demands, but policy measures aimed at reducing these costs are often the first to be sacrificed [5]. For example, the enrollment of migrants fleeing the conflict in Ukraine was later followed by more rigorous identity verification procedures for people seeking to access states in the European Union [3]. A non-adaptive digital divide countermands fairness and anti-discrimination objectives. Systems should therefore commit to the accessibility and usability required to retain participation as technology and technology adoption evolve, acknowledging the effect of these factors on both the digital and physical identities of disabled users[3]. When it is necessary to use a language other than the users' mother tongue, the technology should overcome these limitations [4].

Governance, Oversight, and Legal Frameworks

Complementing the trade-offs between privacy, access, and state capacity, the governance arrangements surrounding digital identity systems encompassing the models, institutions, and tools for oversight and regulation exert a critical influence on these three dimensions[9]. Independent of the specific country context, the governance regime must collectively fulfil three broad functions: set clear legal frameworks and facilitate compliance; supervise the execution of entitlements through monitoring and auditing; and establish mechanisms to investigate and redress complaints and grievances [9]. The relevance of these functions arises because, in particular, countries that are not deploying significant efforts to regulate already collected data have the potential to recover significant state capacity, but installing similar frameworks for digital identity systems could curtail access and privacy at the same time [8]. Governance and implementation arrangements figure prominently throughout the introduction of the ASEAN Smart Cities Network, which seeks to enhance livability, sustainability, and resilience in 26 ASEAN cities through the use of smart solutions. Apart from being developed along the lines of five enabling factors regulatory frameworks, technology, financing, human capital, and partnerships), governance arrangements represent the sixth enabling factor, itself subdivided into four dimensions: institutional mechanisms, regulatory frameworks, stakeholder engagement, and privacy and cybersecurity protocols [10]. Governance and oversight frameworks, alongside more restrictive laws on existing data, fulfil a second function of involving the public. Such measures are instrumental in illustrating the government's capacity to guarantee privacy while collecting data for undisclosed objectives during periods of heightened political sensitivity' [9].

Case Studies and Comparative Perspectives

Evidence from case studies and cross-national comparisons is increasingly guiding the analysis of digital identity systems. Many governments are deploying national digital identity initiatives, with strong support from development banks and aid agencies, while regional arrangements for cross-border identification and data sharing are gaining momentum [7]. Analysis of these initiatives offers insight into trade-offs associated with privacy-preserving designs, accessibility for marginalized groups, and governance models that foster stakeholder accountability [8]. National Digital Identity Initiatives Myanmar, Nepal, and Vanuatu pursued national digital identity initiatives with similar rationale, designs, and reliance on development assistance. Focusing on privacy preservation, equitable access, and institutional accountability highlighted development-related risks that warrant heightened attention [8]. High-level endorsement was not sufficient to ensure data ethics aligned; implementation tangled with domestic politics; and testing, delay, and cost overruns raised operational concerns. Safeguarding ethos–state relations and balancing privacy, this development theme encompasses elements crucial for success in such digital identity programs [6].

National Digital Identity Initiatives

Identity is a universal aspect of life. The overwhelming majority of people in the world are born with captures and records of their information, including photos and fingerprints, and those biometric identifiers are later used in physical or digital identification systems [6]. However, a significant share of the population does not have any form of legal identity, which is essential for accessing a wide variety of services. These people face problems in opening bank accounts, accessing health care services, signing leases, etc.[7]. Without identity, people lack rights, security, and social inclusion, and are very vulnerable to exploitation and violence. Poorly designed or developed identity systems can increase fraud, reduce security, enable or support discrimination, and violate personal integrity, privacy, or dignity [8]. One of the newest changes in identity systems is transitioning to a digital format, which can simplify identity verification processes and reduce operational costs. Such digital identity systems are being developed in many countries [10]. One successful, high-profile case that has garnered global interest is India's Aadhaar system, which captured the data of over 99% of the population in less than a decade.

Open Access
Print ISSN: 2992-6106
Online ISSN: 2992-5789

However, there are still concerns about the system's privacy implications, accessibility for marginalized populations, and compliance with the characteristics of a reliable and usable identity verification mechanism [8].

Cross-Border Identification and Data Sharing

Traditionally, identity verification for international travel has been managed through bilateral agreements to share identity-linked data [9]. These agreements often become outdated and present challenges in reliability and execution. With advances in technology, border crossing is increasingly expected to be a frictionless experience, fueling discussions on collective solutions to cross-border identity verification [7]. The evolution of the Schengen Information System to share identity credentials proportionate to the underlying risks is one example of an emerging multilateral approach [6]. Digital identity systems may facilitate aspects of cross-border identification beyond traditional travel contexts. Some digital identity initiatives are establishing frameworks that augment convenience and security when identifying strangers for physical and online interactions [8]. Verification completeness and data-sharing mechanisms can be proportionately calibrated to the context of use. The current arrangements for online age verification, for instance, share identity attributes only within specific risk-designated contexts. This use case points toward broader multilingual and multi-context digital identity solutions at low to no cost for the user [5].

Lessons Learned and Best Practices

Analysis of national digital identity programs, international identification systems, and cross-border data-sharing mechanisms reveals trends and common pitfalls [10]. Fundamental design principles help policy-makers avoid mistakes and maximize the benefits of digital identity systems [7]. Crucial lessons about the trade-offs between privacy, access, and governance capacity emerge from analysis of different types of identification programs. Across national digital identity systems, a clearer focus on data-minimization principles is required to mitigate concerns about state-sponsored surveillance and abuse of power [8]. Examination of regional cross-border identification systems highlights the importance of searching for common ground across political, institutional, and technological divides when exploring international cooperation for identity recognition [6]. Finally, analyses of transnational data-sharing mechanisms established as part of the response to the COVID-19 pandemic suggest that, even when interoperability is technically possible, legal, ethical, and governance issues can still pose severe obstacles. In particular, a clear articulation of the purpose and uses of cross-border data-sharing initiatives, along with independent systems of oversight and redress, is indispensable to promote trust and ensure accountability [4].

Methodological Considerations

Systems of identification grant access to a variety of resources, whether digital or physical. As compared to the pre-digital era, every identity-related transaction is conducted electronically nowadays [6]. Individuals can provide proof and acquire resources without going in-house and filling out forms. Digital Identity systems simplify such transactions. Such systems have certain advantages [4]. They can ease KYC (Know Your Customer) procedures. When KYC has already been established with a certain service provider and regulatory authority, the same can be shared with another service provider to drop repeated cycle with another provider [1].

Evaluation Metrics for Privacy, Access, and Capacity

Evaluating the privacy, access, and state capacity implications of digital identity systems requires identifying suitable metrics for each outcome [6]. Visitability and interoperability are relevant indicators of privacy, while indicators of trust include systems for verifying and correcting errors and for third-party redress. Acceptance among affected populations should be measured, particularly for marginalized groups; signs of systemic failure should also be identified [4]. The cost-effectiveness of identity verification is a useful proxy for use in the access analysis, which can be further informed by research on the implications of usability, accessibility, and language. Support for user-centric alternatives is another relevant indicator [4]. For the state-capacity dimension, metrics of administrative efficiency, ease of reducing fraud, and transparency of implementation serve as starting points.

The analysis should also consider digital identity systems beyond the national level. Other scales, namely, supranational and subnational, offer their own advantages and weaknesses in fundamentally different ways. Indicators relevant for cross-border identification and data sharing relate to information security [7]. Concurrently, the history of digital identity initiatives in four countries, Australia, Canada, India, and Singapore, can guide the analysis and support the identification of trade-offs, for example, between privacy and state capacity[8].

Data Ethics and Research Gaps

Data collection for evidence-gathering and evaluation should be implemented in a manner consistent with the proposed privacy criteria. Additional privacy concerns arise from the limited consideration of privacy implications across security and development sectors and through the use of business agreements, especially those involving opaque private-sector partners, for cross-border data-sharing and identification arrangements [9]. Moreover, privacy assessment and review processes vary considerably between systems, resulting in considerable variation

Open Access
Print ISSN: 2992-6106
Online ISSN: 2992-5789

across privacy-, access-, and state-capacity-related outcomes [7]. Lack of a shared evaluation framework inhibits comparative assessment of key privacy, access, and state-capacity dimensions. Data-minimization practices, including on-off registration procedures and the use of ephemeral identity tokens, require information gathering at attributes or holders only, indeed, ideally at neither [7]. Security-sensitivities of marginalized communities are rarely fully appreciated; remote verification, especially that linked with consequent algorithmic profiling and surveillance, is often poorly viewed; institutions' failure to adequately explain how systems work diminishes trust in attributes and holders; and redress mechanisms designed primarily for identifiable victims with meaningful deterrent effect remain elusive[6].

Policy Alternatives and Recommendations

Digital identity systems constitute major socio-technical transformations embedded within global digitalisation and economic recovery efforts [9]. They vary in form and function, but have fundamental characteristics in common. Depending on design choices regarding data storage, access, integrity, and user rights, they can differentially accommodate privacy, accessibility, and state-capacity outcomes. All digital identity systems collect identifiable information [8]. If multiple sources of data are aggregated around individuals, those individuals can be profiled in ways that invade privacy and liberty, enabling surveillance by both states and corporations [7]. Each additional data association increases the risk of compromise and misuse, enabling coercive and discriminatory acts ranging from unsolicited persuasion to extortion and violence; therefore, identity systems that centralise personal data increase privacy exposure relative to alternatives [1].

Design Principles for Privacy-Preserving Systems

For digital identity systems to be privacy-preserving, their design should adhere to five principles. First, data minimization entails limiting information collection and storage to the least amount necessary for a given purpose. Second, consent denotes an individual's control over their own data, including whether, when, how, and to whom the data are disclosed [6]. Third, reputable identity providers understand and justify the data they store, and can assure data subjects that the data will not be misused [5]. Fourth, oversight and compliance mechanisms guarantee that the identity system functions jointly with the laws and interests of its users. Finally, redress enables data subjects to receive compensation in the case that misuse occurs, and creates the social conditions that induce identity providers to address complaints seriously [5]. A balance is needed between privacy and the utility of digital identity systems. Complete data minimization is rarely feasible, either because of the need to store supplementary data to validate an identity (for example, an age verification flag) or because equipping administrators with comprehensive user profiles can make their operations both more effective and less intrusive. In other words, there are cases in which it makes sense to break the axiom of data minimization, but the exceptions should be as few and as small as possible [8]. The challenge is to identify and contract those situations, and to withdraw when they are no longer present. The same applies to user consent: while it is more reliable than not having it at all, requiring users to consent to the processing of copious, sensitive data packages makes consent meaningless [9].

Inclusive Access Strategies

The need for digital identity systems to be inclusive is often given rhetorical weight by leaders, yet such commitments remain inadequately translated into action; systems often fall short because of poorly designed policies or the usual difficulties associated with political economy [7]. These issues can be exacerbated by an unwillingness to challenge the global digital divide. More attention is therefore required on access-oriented strategies designed to make systems inclusive, particularly for those falling within the broad definition of marginalized populations [8]. International decision-making bodies such as the International Telecommunication Union have issued calls to close the digital divide, both within and across countries, and the emphasis on inclusive access to identity systems has remained a priority to also support those disproportionately affected by crises and emergencies [6]. Beyond such sentiments, and despite the principle of the core in the UN Roadmap for Digital Cooperation, there has been less focus on practical steps to address the fundamental lack of access to the basic equipment and connectivity needed to gain and use a digital identity [5]. Such barriers cannot be overcome solely by user-centred design principles applied to the interface and experience of the user. Reaching remote and disaster-affected areas with connectivity and digital devices requires significant investment and effort [8].

Governance Models for Accountability

A range of governance models may guide the deployment and oversight of digital identity systems. In Poland, the Ministry of Digitalization is responsible for establishing the architecture and key components of the e-ID system, while the Ministry of Internal Affairs is tasked with verification and issuing identity documents. Within this framework, companies may provide identity services without a license but must employ encryption approved by the Ministry [7]. In France, the Ministry of Economy promulgates an implementation circular for the identity authentication framework and best practices [6]. The National Commission for Information Technology and Civil Liberties is in charge of prior review of privacy-impact assessments and approvals for geolocation services and

Open Access
Print ISSN: 2992-6106
Online ISSN: 2992-5789

privacy-regulated data exchanges. The Commission is also assigned a wide supervisory role on security, quality, management, and the overall implementation of the architecture. In Canada, responsibility for identity management resides with a coordinating Secretariat in the Treasury Board of Canada [8]. In Japan, the National Center of Incident Readiness and Strategy for Cybersecurity advises on the design of secure information systems at national and local levels, as well as systems operated internally by regulatory authorities, such as financial market monitoring and border control for immigration, customs, and quarantine[9]. The Ministry of Internal Affairs operates the My Number system. Local governments manage individual registration for the My Number number, issue identity cards embedded with an IC chip, and provide residents with digital certificates to facilitate user authentication in online transactions. The number is used as an identifier for administrative, tax, and social security purposes as part of a dedicated database, with law enforcement and intelligence organizations authorized to collect and operate designated data [10].

CONCLUSION

Digital identity systems represent a significant transformation in how governments, institutions, and individuals interact within increasingly digital societies. By enabling reliable identification and authentication across a wide range of services, these systems have the potential to improve public administration, expand access to services, and strengthen economic participation. However, the design and implementation of digital identity systems also introduce complex policy challenges related to privacy protection, social inclusion, and state governance capacity. This study has examined digital identity systems through the interconnected dimensions of privacy, access, and state capacity. In terms of privacy, digital identity systems fundamentally reshape how personal data is collected, stored, and shared. The aggregation of biometric, demographic, and transactional data creates opportunities for improved verification and security but also increases the risks of surveillance, profiling, and misuse of personal information. Effective privacy protection, therefore, requires adherence to key principles such as data minimization, informed consent, secure data management, and transparent oversight mechanisms. Strong legal frameworks and independent accountability institutions are essential to ensure that digital identity systems respect individual rights and maintain public trust. Access and inclusion represent another critical dimension of digital identity policy. While digital identity systems are often promoted as tools for expanding access to services, poorly designed systems may inadvertently reinforce existing inequalities. Marginalized populations, including those in remote regions, individuals with limited digital literacy, refugees, and linguistic minorities, often face significant barriers to participation. These barriers may arise from technical requirements, biometric verification failures, language limitations, infrastructure deficits, or lack of trust in institutions. Ensuring inclusive access, therefore, requires user-centered design, multilingual support, flexible verification methods, and targeted outreach to vulnerable populations. Without such measures, digital identity systems risk excluding the very groups they are intended to support. At the same time, digital identity systems can significantly enhance state capacity when implemented effectively. By enabling secure identification across government platforms, these systems can streamline administrative processes, improve service delivery, reduce fraud, and strengthen transparency and accountability. Digital identity infrastructure can support electronic signatures, digital payments, and secure information exchange, allowing governments to deliver services more efficiently and monitor public programs more effectively. Successful examples demonstrate how digital identity systems can contribute to better governance by enabling real-time tracking of transactions, reducing corruption, and strengthening citizen engagement with public institutions. Nevertheless, policymakers must carefully navigate the trade-offs inherent in digital identity design. Systems that prioritize administrative efficiency and comprehensive data collection may compromise privacy protections. Conversely, systems that strongly emphasize privacy safeguards may limit functionality or reduce the ability of institutions to perform essential verification tasks. Similarly, measures intended to prevent fraud or strengthen security may impose burdens that disproportionately affect marginalized populations. Balancing these competing objectives requires evidence-based policymaking, continuous evaluation, and adaptive governance frameworks capable of responding to technological and societal change. Governance and oversight structures play a crucial role in achieving this balance. Effective digital identity systems depend on clear institutional responsibilities, transparent regulatory frameworks, and mechanisms for monitoring system performance and addressing grievances. Independent oversight bodies, privacy regulators, and accountability institutions help ensure that digital identity systems operate in accordance with legal and ethical standards. Public engagement and stakeholder participation further strengthen legitimacy and trust in these systems. Comparative experiences across countries illustrate that digital identity initiatives succeed when they integrate privacy protection, inclusive access strategies, and robust governance mechanisms. Lessons from national and cross-border identity programs highlight the importance of transparency, stakeholder collaboration, and careful management of data-sharing arrangements. As digital identity systems expand beyond national boundaries, international cooperation and standardized protocols for data protection and interoperability will become increasingly important. Future research should continue to explore the social, technological, and governance

Open Access
Print ISSN: 2992-6106
Online ISSN: 2992-5789
implications of digital identity systems. In particular, more empirical evidence is needed to evaluate how different system architectures affect privacy outcomes, inclusion rates, and administrative performance. Interdisciplinary research combining perspectives from public policy, information technology, law, and social sciences will be essential to understanding the broader societal impacts of digital identity initiatives. In conclusion, digital identity systems hold significant promise for improving governance and expanding access to services in the digital era. However, their success depends on careful policy design that balances privacy protection, equitable access, and enhanced state capacity. By prioritizing inclusive design principles, transparent governance arrangements, and strong legal safeguards, governments can harness the benefits of digital identity systems while minimizing risks to individual rights and social equality.

REFERENCES

1. Alpár G, Hoepman JH, Siljee J. *The identity crisis: security, privacy and usability issues in identity management*. Nijmegen (NL): Radboud University; 2011.
2. Hardjono T. A federated authorization framework for distributed personal data and digital identity. *IEEE Commun Mag*. 2019;57(9):88–93. doi:10.1109/MCOM.2019.1800243
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 Network and System Security*. 2010. p. 1–8.
4. Antignac T, Sands D, Schneider G. Data minimisation: a language-based approach (long version). In: *Proceedings of the 29th IEEE Computer Security Foundations Symposium (CSF)*. 2016. p. 1–15. doi:10.1109/CSF.2016.16
5. Manohar A, Briggs J. Identity management in the age of blockchain 3.0. In: *Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP)*. 2018. p. 1–10.
6. Spiliotopoulos T, Tariq Sheik A, Gottardello D, Dover R. Onboarding citizens to digital identity systems. *Gov Inf Q*. 2023;40(2):101800. doi:10.1016/j.giq.2022.101800
7. Elliott K, Coopamootoo K, Curran E, Ezhilchelvan P, et al. Know your customer: balancing innovation and regulation for financial inclusion. *J Financ Regul Compliance*. 2021;29(4):589–604. doi:10.1108/JFRC-05-2020-0065
8. Stephany F. It's not only size that matters: trust and e-government success in Europe [preprint]. 2020. Available from: OSF Preprints.
9. Harbitz ME, Arcos Axt I. *Políticas de identificación y gobernanza: los fundamentos jurídicos, técnicos e institucionales que rigen las relaciones e interacciones del ciudadano con el gobierno y la sociedad*. Washington (DC): Inter-American Development Bank; 2010.
10. Hawn Nelson A, Zanti S. Four questions to guide decision-making for data sharing and integration. *J Public Health Manag Pract*. 2023;29(1):E1–E6. doi:10.1097/PHH.0000000000001572

CITE AS: Lubega Midlage (2026). Digital Identity Systems: Privacy, Access, and State Capacity Outcomes. NEWPORT INTERNATIONAL JOURNAL OF CURRENT RESEARCH IN HUMANITIES AND SOCIAL SCIENCES, 6(1):1-10. https://doi.org/10.59298/NIJCRHSS/2025/61.110000