Digital Public Infrastructure and the Transformation of Public Services

Hannah Whitmore, Karim El-Sayed

Article type: Editorial

Volume 1, Issue 1 (2026)

Read Current Issue →

Abstract

Digital identity, interoperable payments, data-exchange systems, registries, authentication services, and government portals are increasingly described as digital public infrastructure because they provide reusable foundations for public and private services. Their developmental significance, however, depends on more than technical scale. This editorial argues that digital public infrastructure should be evaluated as socio-technical public infrastructure whose effects are shaped by architecture, law, administration, inclusion, privacy, cybersecurity, institutional capacity, and citizen capabilities. Interoperability can reduce fragmentation and transaction costs, but poorly governed identity or data systems can amplify exclusion, surveillance, security risks, and errors across multiple services. Effective systems require privacy-preserving architecture, inclusive identity processes, correction and grievance mechanisms, resilient cybersecurity, accessible service design, transparent governance, and evidence about actual service outcomes. Research should compare institutional models across development contexts and distinguish infrastructure adoption from improved public value. The central question is not whether governments possess digital rails, but whether those infrastructures remain trustworthy, inclusive, interoperable, and correctable as they mediate increasingly consequential interactions between citizens and institutions.

Keywords: digital public infrastructure; digital identity; interoperability; digital payments; e-government; privacy; public services

Citation

Whitmore, H., & El-Sayed, K. (2026). Digital Public Infrastructure and the Transformation of Public Services. Digital Society, Governance & Development, 1(1). https://eldranacademic.com/dsgd/articles/4/

Received	Revised	Accepted	Published
13 April 2026	10 July 2026	14 August 2026	03 September 2026

Copyright

© 2026 Hannah Whitmore, Karim El-Sayed. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) ↗. Use, distribution or reproduction in other forums is permitted, provided the original authors and copyright owners are credited and the original publication in this journal is cited in accordance with accepted academic practice.

Disclaimer

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, the publisher, the editors or the reviewers. Any product evaluated in this article, or claim made by its manufacturer, is not guaranteed or endorsed by the publisher.

1.0 Introduction

1.1 Context and Problem Framing

Digital public services increasingly rely on shared infrastructures rather than isolated departmental websites. Digital identity systems authenticate people across programs; interoperable payment rails support transfers and transactions; data-exchange systems connect registries; electronic signatures enable remote transactions; and service portals integrate interactions that previously required visits to multiple agencies. These systems can reduce administrative duplication, lower transaction costs, and make services available across organizational boundaries. The World Bank defines digital public infrastructure around reusable building blocks such as identification, payments, and trusted data exchange that support digital services across sectors (Clark et al., 2025; World Bank, 2025). UNDP similarly emphasizes foundational systems that enable secure interactions among people, businesses, and governments (United Nations Development Programme, 2024).

The appeal of shared infrastructure is substantial because fragmented digitalization can reproduce the silos of analogue administration. Interoperability allows agencies to reuse verified information, streamline service delivery, and support cross-sector applications. Digital identity can reduce the cost of remote authentication, while digital payments can improve the speed and traceability of transfers. Research on mobile money demonstrates the broader developmental potential of interoperable digital finance: Jack and Suri (2014) found important risk-sharing effects from mobile money in Kenya, and Suri and Jack (2016) documented long-run poverty and gender effects associated with M-Pesa expansion. These findings do not make every digital payment system inclusive, but they illustrate why foundational digital rails can reshape access to services and economic participation.

1.2 Why the Issue Matters

The central tension is that infrastructures amplify both benefits and failures. An identity error in one isolated database may affect one program; an error in a widely reused identity layer may propagate across banking, social protection, health, education, or taxation. A data-sharing architecture can reduce repetitive paperwork but also increase surveillance capacity or expose sensitive information if governance is weak. Digital public infrastructure should therefore be assessed as socio-technical public infrastructure, not simply as software. Its performance depends on interoperability standards, legal safeguards, administrative quality, accessibility, cybersecurity, grievance mechanisms, institutional coordination, and the ability of citizens to understand and correct records that affect them.

2.0 Current Landscape

2.1 Digital Identity

Digital government research has evolved from a focus on online service delivery toward integrated and data-intensive administrative systems. Janowski (2015) describes successive stages of digital-government evolution from digitization toward contextualized transformation, while Margetts and Dunleavy (2013) identify digital-era

governance as a reconfiguration of administrative processes around reintegration, needs-based organization, and digitization. These perspectives are increasingly relevant to infrastructure because shared digital components enable multiple agencies to reorganize service delivery around common systems rather than duplicating identity, payment, or data-management functions.

Digital identity is one of the most widely discussed components. Identification systems can support inclusion when they provide reliable credentials to people who previously lacked formal proof of identity, but their effects depend on enrollment, authentication, data quality, and the ability to correct records. Gelb and Clark (2013) emphasize identification as a development infrastructure, while Whitley et al. (2014) show that identity systems must be understood as information systems embedded in institutional and social relations. Beduschi (2019) highlights privacy, data-protection, and non-discrimination challenges, demonstrating why digital identity cannot be reduced to authentication efficiency.

2.2 Payments

Payments form a second layer. The Global Findex documents the growing importance of digital payments for financial inclusion and government transfers (Demirgüç-Kunt et al., 2022). Mobile-money research demonstrates that low-cost digital transactions can improve risk sharing and economic resilience (Jack & Suri, 2014; Suri & Jack, 2016). DPI initiatives increasingly seek interoperable payment architectures that allow public and private services to transact across multiple providers rather than requiring one closed system.

2.3 Data Exchange

Data exchange and interoperability constitute a third layer. Interoperability can reduce repeated data collection and enable joined-up services, but it also requires common standards, institutional agreements, data governance, and clear authority. Cordella and Bonina (2012) argue that e-government should be evaluated through public value rather than technological efficiency alone, while Bannister and Connolly (2014) show that public values shape how transformative government initiatives should be judged. Twizeyimana and Andersson (2019) similarly synthesize public-value outcomes of e-government across improved services, administration, transparency, ethical behaviour, and broader social value.

2.4 Digital Service Delivery

Recent DPI frameworks attempt to integrate these concerns. The World Bank's approach emphasizes openness, modularity, inclusion, user centricity, privacy, and governance alongside digital building blocks (Clark et al., 2025). International safeguards work likewise increasingly treats inclusion, rights, security, and accountability as architectural requirements rather than downstream corrections.

3.0 Critical Challenges

3.1 Exclusion

Exclusion is one of the most consequential risks because digital infrastructure often becomes mandatory or practically unavoidable. People may be unable to enroll because they lack documents, biometric data may fail for some users, records may contain errors, and authentication may depend on devices or connectivity that users do not control. India's Aadhaar experience illustrates how identification systems can reduce some transaction costs while creating serious concerns about authentication failure, data errors, and access to welfare. Drèze et al. (2017) documented problems in the use of Aadhaar for food-security delivery in Jharkhand, while Khera (2019)

synthesizes broader evidence of design and implementation failures. The lesson is not that digital identity is inherently exclusionary, but that failure rates that appear small statistically can be severe when authentication becomes a gate to essential services.

Privacy and surveillance concerns increase as infrastructures become interoperable. Separate databases create inefficiencies, but their separation can also limit the ease with which information is combined. Data exchange therefore requires purpose limitation, access controls, logging, minimization, and enforceable governance. Beduschi (2019) argues that digital identity creates contemporary challenges for privacy and non-discrimination, while Sullivan (2018) emphasizes the need for ethical approaches to digital identity design. Infrastructure should not make broad data linkage technically easy while leaving lawful purpose and accountability institutionally vague.

3.2 Privacy and Security

Cybersecurity is another systemic challenge. Shared infrastructure can create attractive targets because successful compromise may affect many services simultaneously. Identity providers, payment switches, data-exchange layers, certificates, APIs, and registries require strong security engineering, incident response, redundancy, and recovery. The NIST Cybersecurity Framework 2.0 reinforces governance as part of cybersecurity rather than treating security solely as a technical control set (National Institute of Standards and Technology, 2024). Resilience must include continuity arrangements for periods when authentication, connectivity, or central services are unavailable.

Interoperability itself can fail when standards are incomplete, agencies maintain inconsistent records, or institutional incentives discourage data sharing. Technical interfaces cannot resolve disputes about authority, data ownership, update responsibilities, or legal purpose. Digital government research repeatedly shows that organizational integration is as important as technical integration (Janowski, 2015; Margetts & Dunleavy, 2013). Vendor dependence can compound fragmentation when proprietary interfaces or contractual restrictions make future interoperability expensive.

3.3 Institutional Governance

Grievance and correction mechanisms are often underdeveloped relative to enrollment and transaction systems. A person whose identity data are wrong needs an accessible route to correct them; a failed payment needs investigation and reversal; a wrongly matched record needs an auditable process. These capabilities are fundamental because infrastructure errors can propagate across services. Citizens should not be required to understand which backend system caused an error before they can obtain correction.

3.4 Long-Term Sustainability

Finally, outcome evaluation remains weak. Governments can report numbers of digital identities issued, transactions processed, or services connected, but these indicators do not establish improvements in inclusion, administrative burden, service quality, trust, or welfare. Infrastructure should be evaluated by the public value it enables and by the distribution of benefits and harms across populations.

4.0 Discussion and Priorities

4.1 Integrative Discussion

Digital public infrastructure is best understood as a layered socio-technical system. Technical architecture determines interoperability, latency, security boundaries, and reuse; law defines authorized purposes and rights; administrative institutions determine data quality and service processes; citizens contribute information and

experience errors; and market actors build services on shared rails. Outcomes emerge from the interaction of these layers rather than from infrastructure components in isolation.

This perspective helps explain why interoperability is both valuable and risky. Reuse can reduce repeated verification, accelerate service delivery, and support innovation, but tightly connected systems also increase the reach of bad data, security incidents, or inappropriate surveillance. Modular architecture and strong access controls can reduce some risks, but they must be supported by governance that defines who may access which data, for what purpose, under what oversight, and with what remedies.

Public value offers an important evaluative frame. Cordella and Bonina (2012) argue that information systems in government should be judged according to broader public-value creation rather than narrow efficiency. Twizeyimana and Andersson (2019) similarly demonstrate that e-government value includes service quality, administrative improvement, openness, ethics, and social outcomes. DPI therefore succeeds when infrastructure improves people's interaction with institutions while preserving rights, inclusion, and accountability—not merely when transaction volumes rise.

Institutional capacity is the connecting factor. A technically sophisticated identity platform cannot compensate for poor civil-registration processes, weak grievance handling, inaccessible service design, or inadequate cybersecurity. Conversely, strong governance can make relatively simple infrastructure more trustworthy by limiting data collection, providing alternative channels, and correcting errors quickly. The appropriate design question is therefore not how much infrastructure can be centralized, but how common components can be reused without concentrating unmanageable technical and institutional risk.

Complementary scholarship informing this synthesis includes Donovan (2012); Gelb (2018); Masiero (2021); National Institute of Standards and Technology. (2024); OECD. (2020); United Nations Development Programme. (2024); United Nations Development Programme. (2024); United Nations. (2024); World Bank. (2016); World Bank. (2018); World Bank. (2021); World Bank. (2022); World Bank. (2025); World Bank. (2025); and World Bank. (2025). These works broaden the evidentiary base considered across the field.

4.2 Research and Practice Priorities

A first priority is interoperable but modular architecture. Common standards should support data exchange and service composition without requiring every institution to depend on one monolithic platform. Research should evaluate interoperability not only by successful message exchange but by data semantics, governance, versioning, and resilience across agencies and vendors.

Second, privacy-preserving architecture should be designed into infrastructure. Data minimization, purpose limitation, selective disclosure, strong authentication, encryption, and auditable access should reduce the amount of personal information exposed by routine transactions. Privacy engineering should be evaluated alongside legal governance rather than treated as a substitute for it.

Third, identity systems must be inclusive and correctable. Enrollment procedures should accommodate people with incomplete documentation, disability, limited connectivity, or difficult-to-capture biometrics. Authentication should include proportionate fallback mechanisms where exclusion would cause serious harm. Research should report false rejection, correction time, grievance outcomes, and demographic variation rather than enrollment totals alone.

Fourth, grievance and correction mechanisms should be treated as core infrastructure. Every shared system needs clear institutional ownership of errors, accessible complaint channels, auditable records, and time-bound remedies. These mechanisms should be tested with real users and should not require sophisticated technical knowledge.

Fifth, cybersecurity and resilience require continuous investment. Systems should be assessed under network failure, cyberattack, service-provider outages, credential compromise, data corruption, and dependency failure. National cybersecurity strategies should explicitly address the systemic risks created by shared digital infrastructure (National Institute of Standards and Technology, 2024).

Sixth, outcome evaluation should connect infrastructure to service quality and development. Studies should compare administrative costs, transaction times, exclusion, benefit receipt, financial inclusion, user burden, trust, and distributional effects before and after infrastructure deployment. Digital-payment research demonstrates the value of examining household and welfare effects rather than transaction counts alone (Jack & Suri, 2014; Suri & Jack, 2016).

Finally, comparative research across development contexts is essential. Countries differ in civil-registration coverage, banking systems, administrative capacity, legal safeguards, telecommunications, trust, and state structure. A design successful in one setting may not transfer directly to another. Comparative work should identify which architectural principles generalize and which require local institutional adaptation.

4.3 Implications for the Journal's Scope

Digital public infrastructure research should connect information-systems analysis with public administration, governance, development, economics, cybersecurity, law, and social inclusion. Strong contributions will examine not only architecture but also how systems change service delivery, institutional coordination, citizen burden, privacy, and access to opportunity.

Particularly valuable studies include comparative digital-identity research, interoperability evaluation, payment infrastructure, data-exchange governance, privacy-preserving architectures, cybersecurity and resilience, grievance mechanisms, accessibility, and longitudinal evaluation of service outcomes. Research should distinguish between infrastructure adoption and actual public value; transaction volume, enrollment, or system availability are important but incomplete indicators.

The field also needs evidence from lower-capacity and lower-connectivity environments, where institutional and infrastructural constraints may differ from those assumed in high-income digital-government research. Mixed-method and interdisciplinary studies can help explain why technically similar systems produce different levels of inclusion, trust, or administrative performance. Rigorous research should make both benefits and failure modes visible so that infrastructure can be improved without turning digitalization into an end in itself.

4.4 Conclusion

Digital public infrastructure can change how citizens authenticate, receive payments, share information, and obtain services, but its developmental consequences are not determined by technical architecture alone. Shared digital rails can reduce fragmentation and transaction costs while simultaneously magnifying identity errors, cybersecurity incidents, exclusion, or inappropriate data use across many institutions.

The appropriate standard is therefore socio-technical performance. Infrastructure should be interoperable enough to enable reuse, modular enough to avoid unnecessary concentration, secure enough to withstand systemic threats, inclusive enough to serve people with diverse capabilities, and governable enough to provide correction and accountability. These qualities require coordination among engineers, administrators, legal institutions, service providers, and the public.

Digital transformation should ultimately be judged by the quality of institutional interaction it enables. A successful infrastructure is not one that merely issues the most credentials or processes the most transactions; it is one that reduces burdens, expands access, preserves rights, survives disruption, and allows errors to be corrected

without imposing disproportionate costs on citizens. The future of digital public infrastructure will therefore depend as much on governance and institutional capacity as on software, standards, and networks.

5.0 Declarations

5.1 Author Contributions

Dr. Hannah Whitmore and Dr. Karim El-Sayed contributed to the conceptual development, literature synthesis, critical interpretation, drafting, and revision of the editorial.

5.2 Funding

No external funding was received for the preparation of this editorial.

5.3 Competing Interests

The authors declare that they have no conflicts of interest or competing interests relevant to this editorial.

5.4 Data Availability

No original datasets were generated or analysed for this editorial.

5.5 AI Use Disclosure

Generative AI was used to support literature organization and language drafting during preparation of this editorial. The authors remain responsible for independently verifying the accuracy of the arguments, citations, references, and final submitted text in accordance with the publisher's policy.

6.0 References

Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: A framework and programme for research. Government Information Quarterly, 31(1), 119–128. https://doi.org/10.1016/j.giq.2013.06.002

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2). https://doi.org/10.1177/2053951719855091

Clark, J., Marin, G., Ardic Alper, O. P., & Galicia Rabadan, G. A. (2025). Digital public infrastructure and development: A World Bank Group approach. World Bank.

Cordella, A., & Bonina, C. M. (2012). A public value perspective for ICT enabled public sector reforms: A theoretical reflection. Government Information Quarterly, 29(4), 512–520. https://doi.org/10.1016/j.giq.2012.03.004

Demirgüç-Kunt, A., Klapper, L., Singer, D., & Ansar, S. (2022). The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19. World Bank. https://doi.org/10.1596/978-1-4648-1897-4

Donovan, K. (2012). Mobile money for financial inclusion. In T. Kelly & C. Rossotto (Eds.), Information and communications for development 2012: Maximizing mobile (pp. 61–73). World Bank.

Drèze, J., Khalid, N., Khera, R., & Somanchi, A. (2017). Aadhaar and food security in Jharkhand: Pain without gain? Economic and Political Weekly, 52(50), 50–59.

Gelb, A., & Clark, J. (2013). Identification for development: The biometrics revolution. Center for Global Development Working Paper 315. Center for Global Development.

Gelb, A., & Diofasi Metz, A. (2018). Identification revolution: Can digital ID be harnessed for development? Center for Global Development.

Jack, W., & Suri, T. (2014). Risk sharing and transactions costs: Evidence from Kenya's mobile money revolution. American Economic Review, 104(1), 183–223. https://doi.org/10.1257/aer.104.1.183

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. Government Information Quarterly, 32(3), 221–236. https://doi.org/10.1016/j.giq.2015.07.001

Khera, R. (2019). Aadhaar failures: A tragedy of errors. Economic and Political Weekly, 54(14), 38–42.

Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: A quasi-paradigm for government on the Web. Philosophical Transactions of the Royal Society A, 371(1987), 20120382. https://doi.org/10.1098/rsta.2012.0382

Masiero, S., & Bailur, S. (2021). Digital identity for development: The quest for justice and a research agenda. Information Technology for Development, 27(1), 1–12. https://doi.org/10.1080/02681102.2021.1859669

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

OECD. (2020). The OECD digital government policy framework: Six dimensions of a digital government. OECD Public Governance Policy Papers, No. 2. OECD Publishing. https://doi.org/10.1787/f64fed2a-en

Sullivan, C. (2018). Digital identity—From emergence to ethical identity. Computer Law & Security Review, 34(4), 723–743. https://doi.org/10.1016/j.clsr.2018.05.041

Suri, T., & Jack, W. (2016). The long-run poverty and gender impacts of mobile money. Science, 354(6317), 1288–1292. https://doi.org/10.1126/science.aah5309

Twizeyimana, J. D., & Andersson, A. (2019). The public value of E-Government—A literature review. Government Information Quarterly, 36(2), 167–178. https://doi.org/10.1016/j.giq.2019.01.001

United Nations Development Programme. (2024). Digital public infrastructure. UNDP.

United Nations Development Programme. (2024). Universal safeguards for digital public infrastructure. UNDP.

United Nations. (2024). Global Digital Compact. United Nations.

Whitley, E. A., Gal, U., & Kjaergaard, A. (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. European Journal of Information Systems, 23(1), 17–35. https://doi.org/10.1057/ejis.2013.34

World Bank. (2016). Identification for development strategic framework. World Bank.

World Bank. (2018). Principles on identification for sustainable development: Toward the digital age. World Bank.

World Bank. (2021). World development report 2021: Data for better lives. World Bank.

World Bank. (2022). GovTech maturity index, 2022 update: Trends in public sector digital transformation. World Bank.

World Bank. (2025). Digital delivery systems for social protection. World Bank.

World Bank. (2025). Digital government. World Bank.

World Bank. (2025). Digital public infrastructure and services. World Bank.