Digital Infrastructure Solutions to Empower Citizens: A Toolkit for Policymakers

Designing, Scoping and Governing Digital Infrastructure to Advance Data Agency

May 2025

Project Liberty Institute //

GLOBAL SOLUTIONS
THE WORLD POLICY FORUM

This report draws on a series of multistakeholder consultations held on November 12, 2024, on the sidelines of the Paris Peace Forum and in the lead-up to the AI Action Summit, as well as on March 31, 2025, at Georgetown University in Washington, DC. It captures key discussions on the development and deployment of digital infrastructure, with a focus on how governments can foster innovation in this space. While every effort has been made to accurately reflect the input provided, the views expressed in this report are those of the Project Liberty Institute and the Global Solutions Initiative. They do not necessarily represent the positions of the organizations with which participants of the consultations are affiliated.

Please cite as Nicole, S., Mishra, V., Bell, J., Kastrop, C., Rodriguez, M. (2025, May). Digital Infrastructure Solutions to Empower Citizens: A Toolkit for Policymakers. Project Liberty Institute & Global Solutions Initiative.

Project Liberty Institute //

About Project Liberty Institute

Project Liberty Institute is a 501(c)(3) organization that serves as an international meeting ground for technologists, policymakers, entrepreneurs, investors, academics, civil society, and governance experts. Its mission is to advance responsible governance and evidence-based innovation across entrepreneurship, infrastructure, and capital allocation, shaping frameworks for how we design, invest in, deploy, and govern new technologies. The Institute supports timely, actionable research on digital technology and responsible innovation. Its academic partners include Stanford University, Georgetown University, Harvard, MIT and other leading institutions.

Central to Project Liberty Institute's mission is the stewardship of the Decentralized Social Networking Protocol (DSNP), a public- interest infrastructure protocol available as a public utility. DSNP supports a new era of innovation that empowers people over platforms and serves the common good.

Through its multifaceted approach, Project Liberty builds solutions to help people reclaim control of their digital lives, fostering voice, choice, and stake in a better internet.

GLOBAL SOLUTIONS
THE WORLD POLICY FORUM

About Global Solutions Initiative

The Global Solutions Initiative (GSI) is an independent, non-profit platform bringing together international think tanks, civil society organizations, researchers, policymakers, and business leaders to develop evidence-based solutions to global challenges. Founded during Germany's G20 Presidency in 2017, GSI leverages its networks and regional hubs to foster dialogue and collaboration in support of the G7, G20, and other multilateral processes.

A key focus of GSI's work is the transformative potential of digital technologies and AI. GSI addresses critical challenges such as inequitable digital governance, lack of data privacy, and the risks posed by advanced AI systems, while exploring opportunities for human-centered innovation. Together with key stakeholders, GSI works to develop frameworks for responsible AI, empower users with greater control over their data, and design inclusive digital infrastructure to drive equitable social and economic progress.

Authors

Project Liberty Institute

Jeb Bell
Head of Strategic Insights

Sarah Nicole
Policy & Research Manager

Global Solutions Initiative

Christian Kastrop
CEO & Partner

Vidisha Mishra
Director, Global Outreach & Policy

Mateo Rodriguez
Assistant to the CEO & Strategic Outreach Manager

The authors would like to particularly thank Sumedha Deshmukh and her thoughtful feedback on this toolkit.

Experts Consulted for this Initiative

First Consultation in Paris on November 12, 2024

Paul Ash
Chief Executive, Christchurch Call Foundation

Amir Banifatemi
Director, AI Commons

Renato Berrino
Research Manager, Open Data Charter

Matthias De Bievre
President, Prometheus-X

Constance Bommelaer de Leusse
Executive Director Technology & Global Affairs Innovation Hub Sciences Po Member of the 2025 AI Action Summit Steering Committee

Luzius Cameron
CEO, SCION Association

Siméon Campos
Executive Director, Safer AI

Duncan Cass-Beggs
Executive Director of Global AI Risks Initiative, Centre for International Governance Innovation

Benjamin Derothe
Parliamentary Assistant, French Senate

Gilles Fayad
Expert, GPAI/OECD

Paul Fehlinger
Director of Policy, Governance Innovation & Impact, Project Liberty Institute

Emma Ghariani
Head of the Open Source and Digital Commons Division, French Interministerial Digital Directorate

Julie Inman Grant
eSafety Commissioner, Australian eSafety Commissioner

Konstantinos Karachalios
Former Executive, IEEE

Innar Liiv
Professor of Big Data & Member of Senate, Tallinn University of Technology

Nicole Manger
Lead - Global AI Governance & Digital Cooperation, Federal Foreign Office of Germany. Fellow of Practice, TUM Think Tank - Technical University of Munich

Gilles Mentré
Co-founder, Electis

Francesca Musiani
Research Professor - Co-Founder & Deputy Director, Center Internet, and Society, CNRS

Helge Sigurd Naess-Schmidt
Director, Næss-Schmidt Advisory Fellow, Global Solutions Initiative

Corinne Narassiguin
Senator, French Senate

Kasia Odrozek
Director, Insights, Mozilla

Gabriela Ramos
Assistant Director-General for Social and Human Sciences, UNESCO

Ellen Read
Chief Engagement Officer, Christchurch Call Foundation

Mercedes de los Santos
Project Director, Open Data Charter

Dr. Mehdi Snene
Senior Advisor on AI, UN Office of the Secretary-General's Envoy on Technology

Experts Consulted for this Initiative

Second Consultation in Washington, D.C. on March 31, 2025

Shinnola Alexander
Policy Advisor, US House of Representatives

John Beezer
Senior Advisor, US Senate, Commerce Committee

Tony Bishop
Senior Advisor, Office of the National Cyber Director, Former White House Advisor

Grace Brightbill
Legislative Assistant, Congressman Don Beyer

Joel Burke
Policy Analyst, Mozilla

Laura Caroli
Senior Fellow, Center for Strategic and International Studies

Julie Cohen
Mark Claster Mamolen Professor of Law & Technology, Georgetown Law

Delara Derakhshani
Director of Policy and Partnerships, Data Transfer Initiative

Renee DiResta
Associate Research Professor, McCourt School of Public Policy

Ariana Fowler
Head of Research, EQTY Lab

Adrienne Goldstein
Senior Program Coordinator, German Marshall Fund

Laura Halenius
Senior Lead, The Finnish Innovation Fund Sitra

Jack Henderson
COO, RadicalxChange Foundation

Margaret Hu
Professor of Law, William & Mary Law

Akash Kapur
Visiting Research Scholar, Princeton / New America

Mallory Knodel
Executive Director, Social Web Foundation

Miapetra Kumpula-Natri
Member of the Parliament, Parliament of Finland

John Perrino
Senior Policy and Advocacy Expert, Internet Society

Sanjay Patnaik
Director, Center on Regulation and Markets, The Brookings Institution

Matthew Victor
Project Director, MA Platform for Legislative Engagement, Attorney, Bernstein Shur

Jordan Sandman
Principal, Investments, Co-Develop

Alex Scheuer
Policy Advisor, Democratic Leader Jeffries

Lisa Singh
Director, Massive Data Institute, Georgetown University

Joshua Silver
Attorney, Bernstein Shur

Lacey Strahm
Head of Policy, OpenMined

Richard Whitt
President, GliaNet Alliance

Jonathan Wolfe
CTO, MeWe

Chinasa T. Okolo
Fellow, The Brookings Institution

Cameron Smith
Military Legislative Assistant, U.S. Senate

Foreword

The stakes for digital infrastructure have never been higher. Rapid advances in technology – in particular, generative AI – are not only transforming the nature of work and everyday life but redefining the meaning of sovereignty for individuals, communities and even nation states. This toolkit is meant to assist policymakers in designing digital infrastructure that can keep pace with emerging technologies, while preserving basic rights and rules that protect and empower individuals as productive members of society.

The toolkit draws on insights from a series of expert, multistakeholder dialogues convened on the sidelines of the Paris Peace Forum on November 12, 2024 and the Decentralized Tech Summit in Washington, DC, on March 31, 2025. It is also informed by a panel discussion at the Think7 Summit in Waterloo, Canada, on April 2, 2025 and individual interviews. An intermediary report,[1] released in December 2024, captured comments and observations shared at the first consultation in Paris.

Inspired by Project Liberty Institute's *Fair Data Economy Task Force Recommendations*[2] and informed by the Global Solutions Initiative's extensive experience engaging member states and engagement groups of the G7 and G20, the toolkit assumes that digital infrastructure is too vital a resource to be left in the hands of for-profit, proprietary interests. Governments must ensure that this bedrock of the digital economy, from energy supply to data capacity to data rights, is designed, resourced and governed to encourage opportunity, innovation and prosperity.

While the toolkit is focused on assisting policymakers, its ultimate stakeholders are citizens themselves. If given a meaningful voice, choice and stake in the digital economy, individuals can spark technological innovation, drive economic growth and strengthen societal well-being. Digital infrastructure is a foundation for a better world and a better tomorrow.

1. Nicole et al., "Digital Infrastructure Solutions to Advance Data Agency in the Age of Artificial Intelligence."

2. Fehlinger, Paul, Jeb Bell, Claire McBride, and Maria Farrell. "'Toward a Fair Data Economy: A Blueprint for Innovation and Growth.'" Project Liberty Institute, 2024.

Executive Summary

While government initiatives drove the creation of the global internet, for decades, governments have largely adopted a passive, or at best reactive, posture as commercial interests have shaped the digital economy – including the rights, rules, and protections that define how citizens participate in economic, social and even civic life. If governments are to become more agile and keep pace with technological change, this situation must change. One answer is for policymakers to direct their attention to the foundations of today's – and tomorrow's – economy: digital infrastructure.

Digital infrastructure encompasses not only physical elements like broadband networks, data centers, and cloud services but also the laws, standards, and protocols that govern transparency, access and control of data. By developing comprehensive, long-term strategies for the design, scope and governance of digital infrastructure, governments can influence the social, economic and civic impact of new technologies, as they emerge rather than after the fact.

This toolkit is intended to help governments reassert authority over digital infrastructure, while simultaneously encouraging innovation and empowering citizens. It walks policymakers through a four-stage process, highlighting key questions, considerations and trade-offs that can affect the degree to which digital infrastructure is trusted, used and responsive to the needs of citizens and society.

Below is a brief description of each toolkit stage:

Assess
Conduct a holistic diagnostic evaluation of current digital infrastructure, institutional capabilities, governance frameworks, and gaps. This step emphasizes the importance of leveraging existing strengths and identifying clear areas for strategic intervention.

Design
Make deliberate, strategic choices about infrastructure openness (closed versus open systems), scope (global versus local standards), and governance structures (centralized versus multistakeholder models). Successful infrastructure solutions often employ hybrid models that balance open standards with robust governance and security measures.

Safeguard
Implement essential cross-cutting safeguards such as transparency, accountability mechanisms, inclusive stakeholder engagement, rights-based frameworks, data governance standards, resilience planning, and whistleblower protections. These safeguards are critical to ensuring infrastructure remains equitable, secure, and responsive.

Adopt
Foster citizen engagement through digital literacy initiatives and awareness campaigns to ensure meaningful use and trust in digital infrastructure. Addressing widespread data illiteracy and promoting user-centered design are essential for ensuring infrastructure adoption and efficacy.

Ultimately, this toolkit empowers governments to shift from passive or reactive approaches to proactive governance and strategic investment, enabling the creation of inclusive, resilient digital infrastructures that promote equitable growth, protect citizens' rights, and foster innovation.

Digital Infrastructure, Data Agency and Governments as Market Shapers

Digital infrastructure underpins the economy of today – and tomorrow: from broadband networks, data centers, cloud services, to the protocols and standards that ensure interoperability of tech platforms, services and systems. How digital infrastructure is designed affects the degree to which economic power is concentrated or distributed, innovation stifled or encouraged, and prosperity available to the few or the many.

Governments are just now beginning to grapple more systematically, and strategically, with digital infrastructure solutions intended to serve the public interest and reduce the influence of commercial actors who have traditionally dominated the design and delivery of such infrastructure. Some recent examples showcase varied models of design, governance, and funding. As the table below illustrates, not all of these solutions have been successful, but offer crucial insights on the direction for future policy pathways.

Digital infrastructure solutions: Success is not always guaranteed

Govern-ment	Initiative	Status	Approach
Taiwan	DIGI+	Ongoing	Managed intersectionally, with collaboration across ministries, civil society, and the private sector. Integrated digital inclusion, cybersecurity, open data, and citizen engagement.
Kenya	Huduma Namba	Suspended	Worked in silos with minimal public consultation, privacy and inclusion concerns. Faced legal challenges, opposition from civil society, and exclusion of marginalized groups; rollout paused several times.
Mexico	Mexico Conectado	Suspended	Lack of sustainable funding and weak inter-agency collaboration. Initially promising (nearly $1 billion budget), but halted due to various political transitions and inconsistent support.

Data Agency as a Path Toward Digital Sovereignty

One of the hallmarks of Taiwan's successful digital infrastructure solution has been the inclusion of multiple voices, including those of citizens. Implicit in the Taiwan example is the belief that people should have a say in how their data is used. This is the principle of data agency. If governments are to empower citizens to be drivers of innovation, engaged employees, trusting consumers, and responsible members of society, enabling data agency through digital infrastructure would seem essential.

Data agency may not be the most obvious framework that policymakers could adopt when designing digital infrastructure. There is a compelling argument that infrastructure, as a fundamental layer of the technology stack, should be a building block of "digital sovereignty" – that is, the ability of national governments, in particular, to define the rules and standards for their geographic "slice" of the global digital economy. Data agency and digital sovereignty, however, do not need to be at odds.

Traditionally, the quest for digital sovereignty has frequently trapped governments in a reactive mode: responding to technological developments after the fact and relying almost exclusively on regulation to rein in the perceived harms or excesses of private sector innovation. One need look no further than the current Meta antitrust trial in the United States – more than a decade after the company acquired Instagram and Whatsapp – to appreciate the inefficiency and ineffectiveness that can plague governments as they try to play catch-up with changes in the technology sector.

Intervening at the infrastructure layer – and ensuring that citizens enjoy data agency – offers a path toward a more strategic, agile and resilient form of digital sovereignty. By designing the physical and legal foundations of the digital economy, governments position themselves as shapers of technology, influencing the latest innovations as they emerge, rather than after the fact. In addition, by empowering citizens through basic data rights, governments can create a more inclusive and equitable playing field for workers, entrepreneurs and small- and -medium-sized businesses.

In essence, a focus on ensuring data agency at the infrastructure layer of the technology stack transforms governments from reactive market regulators to pro-active market shapers. Of course markets – and the digital economy – are global today. To fully succeed as market shapers, governments should be mindful of the advantage that comes from aligning data-agency standards across multiple jurisdictions, rather than only locally. Otherwise, the centralized, coordinated power of global technology companies may yet deprive states of their digital sovereignty. Fundamental, and universal, principles and rights of data agency empower both governments and citizens.

If fully realized, the ability of governments to shape and enforce rights-based digital regulation would reaffirm an open, competitive global market while ensuring countries retain the authority to: (1) promote their own tech-related specialisms, at home and abroad, and (2) intervene when global tech forces threaten the rule of law, public accountability, or other national interests. This is a vision of sovereignty grounded in resilience and shared norms, not the isolation and rigidity that accompany quests for data localization or digital autarky. A total self-reliant infrastructure stack or "full technological sovereignty" is neither realistic nor desirable.

Digital Infrastructure Fundamentals

In order for governments to successfully position themselves as market-shapers, digital infrastructure must be conceived and addressed at the ecosystem level. The narrow IT solutions often pursued by governments will not suffice[3]. For example, the establishment of a digital identity system, while important, does not in itself constitute a digital infrastructure strategy. A truly strategic approach addresses the foundational systems that enable interoperability, data portability, and user control across sectors. It is about rethinking infrastructure not just as a tool for government service delivery, but as a layer that empowers individuals to manage and use their data—including data generated outside the purview of the state.

As suggested above, this is not just about hardware. Infrastructure also includes the rules and standards that shape how systems interact: the protocols for data exchange, authentication, and governance. These less visible elements are just as critical as the fiber optic cables and server farms. Without common standards and open protocols, digital systems become fragmented, duplicative, and expensive – a reality numerous governments have come to recognize after years of siloed IT investments.

Just as it is critical for governments to take a comprehensive approach to digital infrastructure, it is also important to differentiate interventions at the infrastructure layer from those at the app layer. Platform-level interventions, like cookie banners or app-based privacy settings, cannot solve deeper structural imbalances around data control and digital power. True transformation requires building public capacity into the foundation of the digital economy. By focusing on the fundamentals of the infrastructure layer – such as internet service providers (ISPs), data centers, cloud systems, and standards/protocols, etc. – governments can create the conditions for inclusive, dynamic economies, as well as agile governance.

3. Bartley, "The Economics of Shared Digital Infrastructures | Bartlett Faculty of the Built Environment."

Governments as Market Shapers

In this context, rather than trying to control every layer of the technology stack – from energy sources to microchips – governments should act as market-shapers, focused on the critical intersection where physical infrastructure meets public governance. This includes data centers, cloud computing, and digital identity frameworks – paired with the rules and norms that ensure these systems serve the public interest.

Just as investments in roads or power grids yield long-term benefits by creating new markets and improving efficiency, digital infrastructure is a strategic asset that modernizes governance and drives economic growth. Enhanced digital infrastructure equips the private sector with standardized, interoperable platforms that not only lower entry barriers and integration costs but also pave the way for innovative business models and new revenue opportunities. Estonia's X-Road and the India Stack, especially during COVID-19, exemplify how robust infrastructure can expand access to services, foster economic participation, and drive data-based solutions for societal challenges while fostering innovation through open standards.[4]

As market shapers, and not merely regulators, governments are uniquely positioned to guide the future digital economy. By taking a proactive role in funding, developing and deploying digital infrastructure, governments can advance their own technological expertise and capacity – positioning themselves to be more effective advocates for the public interest.

Government alone, however, cannot guarantee that digital infrastructure meets the needs of citizens or facilitates inclusive, dynamic economic growth. Civil society and multistakeholder oversight are essential, not just as a check on state power, but as co-creators of a digital future rooted in transparency, inclusivity, and public interest. Again, the principle of data agency – giving people a meaningful voice, choice and stake in the digital economy – is critical to creating digital infrastructure that creates robust digital sovereignty, while shaping, rather than constraining, technological innovation.

4. "How Estonia Fights Covid-19 by Going Online."

The Toolkit

This toolkit[5] for policymakers offers a practical, adaptive framework to help governments move from fragmented, reactive digital interventions to strategic, long-term stewardship of digital infrastructure as a public good. It does not prescribe one-size-fits-all solutions because national needs, capacities, and political economies differ. Instead, this toolkit is a starting point: a flexible guide to help policymakers ask the right questions, make informed trade-offs, and adapt frameworks to their own institutional realities.

The toolkit offers a structured but flexible four-stage process—assess, design, safeguard, and adopt—to guide national and multilateral strategies. Rather than prescribing a single model, it supports governments in navigating trade-offs around openness, sovereignty, interoperability, and innovation, all while adapting to their unique national and institutional realities.

Importantly, the toolkit is modular: governments do not need to follow all four stages in sequence—they might already have completed one stage, or they may realize partway through that a project should not proceed.

// Assess Identify existing infrastructure, institutional strengths, governance gaps, and critical bottlenecks. This stage helps governments avoid duplication, repurpose what works, and focus investment where it matters most.

// Design Make intentional decisions about system architecture: Who governs it? Who can access or contribute to it? How open or interoperable should it be? This stage helps governments navigate trade-offs between control and innovation, sovereignty and collaboration.

// Safeguard Embed foundational protections—such as transparency, interoperability, accountability, rights-based frameworks, and resilience-by-design. These safeguards ensure that infrastructure remains equitable, secure, and responsive even as technologies evolve.

// Adopt Infrastructure only works if people use and trust it. This stage focuses on driving adoption through digital literacy, inclusive design, and civic engagement. It recognizes that infrastructure must be human-centered to achieve meaningful scale and legitimacy.

Crucially, it supports alignment across key agendas such as digital and financial inclusion, infrastructure investment, data governance, and resilient public services—making it a powerful resource for G7/G20 coordination and priority-setting. As global policymakers confront mounting pressures to build digital systems that are secure, trusted, and inclusive, this toolkit provides a shared, outcome-oriented starting point for action.

5. See definition in the Appendix

Step 1: Assessing

When tackling systemic and comprehensive reforms, governments often assume they must build digital infrastructure from scratch. But in many cases, that assumption doesn't hold. A more cost-efficient approach begins by mapping what already exists. Many countries have made significant investments in digital systems, but progress is often uneven. In some contexts, robust broadband networks, universal broadband access, or national digital ID systems are already operational, yet data governance remains fragmented or underdeveloped. Elsewhere, technical capacity may be strong, but horizontal coordination and long-term planning are limited.

The first step is a sober, systems-level assessment. Rather than approaching digital development through isolated projects, governments should adopt a comprehensive vision that considers existing infrastructure, institutional capabilities, and gaps across the digital ecosystem. That vision must also account for long-term sustainability—not just initial deployment.

A common challenge in public infrastructure initiatives is the imbalance between the excitement of launch and the unglamorous but essential work of maintenance. In the digital domain, neglecting upkeep can have real consequences: poor data quality undermines service delivery, excludes users, and worsens with automation. For instance, slight discrepancies in name records across systems can lock individuals out of vital services. Ensuring data integrity and system functionality over time requires not only robust processes but also durable funding structures—beyond one-off project budgets—to support ongoing governance, quality assurance, and maintenance.

Key Diagnostic Questions for Policymakers

Questions	Objective
What digital infrastructure assets already exist, and who governs them?	To map the current ecosystem and identify existing capacities and responsibilities.
Where are the critical gaps, technical, legal, or institutional, that hinder scalability or interoperability?	To pinpoint bottlenecks preventing integration or broader usage.
What is the exact scope of the digital infrastructure solution proposed?	To clarify what is the exact purpose of the infrastructure, sometimes it might benefit from being very limited to scale faster.
Do current systems prioritize data protection, privacy, and public trust?	To evaluate whether foundational values are embedded in design and governance.
Are digital services inclusive, accessible, and responsive to all users, particularly marginalized groups?	To assess equity and responsiveness in service delivery.
How is digital infrastructure funded, maintained, and evaluated? Is the model sustainable?	To ensure long-term viability and responsible stewardship of infrastructure assets.
Is there a clear and coordinated digital strategy across ministries and government levels?	To assess horizontal and vertical alignment across the public sector.
At each phase, can we identify when government leadership adds value, and when it might not be needed?	To guide role clarity and strategic public-private collaboration.
Is a digital infrastructure solution here really needed?	To assess whether there will be a real adoption of the created services.

The final question is critical. Effective public digital infrastructure hinges on governments continuously assessing when to intervene and when to step back.[6] This shift requires moving from project-based execution to infrastructure-based thinking, i.e. digital tools can no longer be treated as temporary, siloed solutions. Instead, they must be governed as durable public goods requiring coordination across ministries, jurisdictions, and private-policy domains. A key barrier is the failure to treat digital as infrastructure per se: a foundational layer enabling interaction across sectors, very much so like the analogue world infrastructure (roads, bridges etc.). While initiatives like India Stack and Eurostack point in the right direction, conventional tools like cost-benefit analysis fall short in capturing the long-term, systemic value of digital infrastructure.[7]

In this context, the three principles to effectively assess and guide the development of digital infrastructure are:

// Trust: Systems must be secure, transparent, and accountable. Without trust, there is no large-scale adoption.

// Usefulness: Infrastructure must deliver value, efficiency, and impact. Without usefulness vis a vis context, it becomes irrelevant.

// Responsiveness: Systems must evolve, adapt, and be informed by real-world needs. Without responsiveness, legitimacy erodes.

These principles offer a framework for governments to not only build effective digital infrastructure but also ensure it is politically, socially, and economically sustainable, and most importantly allows for adoption.

Looking Ahead: Navigating Tradeoffs

As governments take a more proactive role, they will encounter unavoidable tradeoffs— those between regulation and innovation are for instance the most frequently cited. These tradeoffs are not zero-sum but exist along a spectrum. They span three core domains: technology design, scoping, and governance models. The key task for policymakers is not to eliminate these tensions but to manage them transparently, balancing public interest with technological progress.

The following sections offer a practical, foundational toolkit to guide the journey—helping governments navigate complexity, make principled decisions, and build inclusive, resilient, future-ready digital infrastructure. Governments may place themselves differently across the three tradeoffs, and positions may shift over time. With ongoing innovation, the listed options represent broad categories, not exhaustive choices—helping governments locate themselves and trace a path forward.

6. Metagov Seminar - Digital Public Infrastructure to Unlock Each Person's Economic Potential (Rowan).

7. Bartley, "The Economics of Shared Digital Infrastructures | Bartlett Faculty of the Built Environment."

Step 2: Designing, Scoping, Governing

Designing digital infrastructure means making strategic choices about power, access, and accountability. While the spectrum from closed to open offers a helpful conceptual map, policymakers must translate these strategic tradeoffs into concrete design choices. This requires asking the right diagnostic questions – ones that interrogate not just the technical architecture, but also the political incentives, institutional capacities, and societal needs that shape it. The questions below help surface those tradeoffs – turning abstract values into practical design moves that shape how infrastructure works, for whom, and to what end.

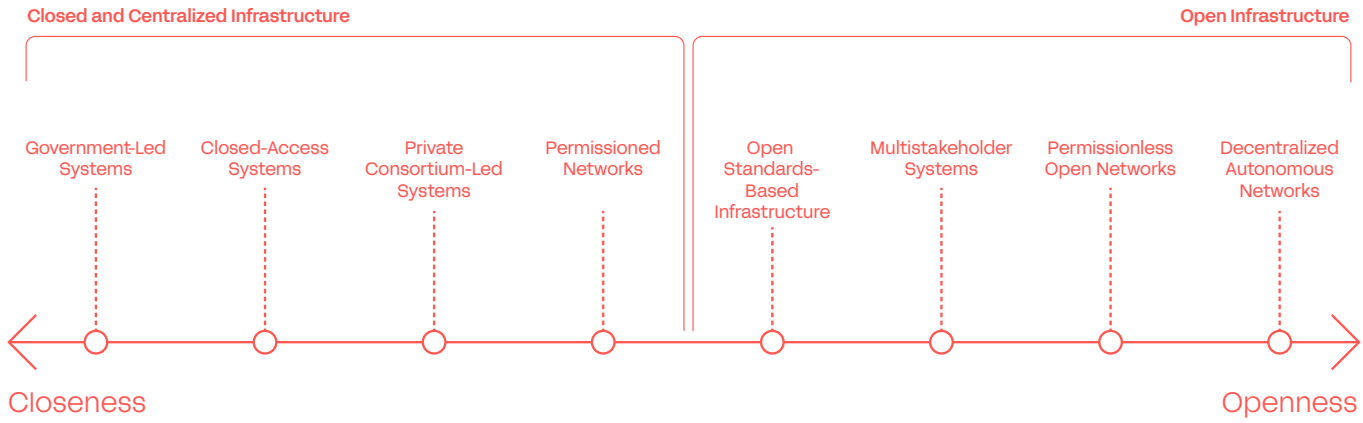
Key Diagnostic Questions for Policymakers

Design Models	Questions
Strategic Foundations See Section 2.1	What are the long-term political and economic goals this infrastructure must support? Is the infrastructure being treated as a strategic national asset or as a tactical service solution?
Governance and Access See Section 2.3 for more	Who is the final point of appeal, and how is that control structured and held accountable? Is governance centralized, federated, or distributed – and what are the implications of that choice? Which actors (public, private, civil society, international) have access to build on, contribute to, or govern the system?
Openness and Interoperability See Section 2.1 and Section 2.2 for more	Where can open standards be adopted to maximize interoperability and adaptability? What mechanisms ensure that openness does not compromise security or sovereignty? Is the system interoperable with other national or global frameworks, including trade, finance, and data governance systems?

Data Use and Protection	What types of data should be made open, and what should remain confidential or restricted? Who decides, and through what process, what data is available, and under what conditions (e.g., licensing, consent, reciprocity)? How are data classification and access decisions governed – and are these processes transparent and contestable?
Trust and Resilience See Section 3	What redress mechanisms exist for harm caused by data misuse or breaches? How does the infrastructure support auditability, transparency, and public oversight? How can public trust be built into system design – especially in contexts of low institutional confidence? What redundancies and fallback mechanisms exist to ensure continuity under stress or failure?
Innovation	Does the infrastructure design allow for third-party innovation without compromising system integrity? How does openness enable localized or sector-specific innovation (e.g., fintech, agriculture, health)?

2.1 Design: Navigating the Spectrum from Closed to Open Digital Infrastructure

At the heart of digital infrastructure design lies a critical tradeoff: **openness vs. closed**. Whether to build systems that are tightly governed or widely participatory is not just a technical decision – it's a political and strategic one. This first tradeoff is also the most comprehensive one. Each model comes with its own implications for sovereignty, innovation, resilience, and public trust.



Design Options Along the Openness Spectrum

Approach	Description	Use Case Examples
Government-Led Systems	Fully controlled and operated by the state, with centralized decision-making and oversight.	Cuba's state-owned telecom, ETECSA.[8]
Closed-Access Systems	Infrastructure is controlled by a single entity with no third-party participation. Typically streamlined but not open to external input.	Starlink: vertically integrated, no external access or service-layer integration.[9]
Private Consortium-Led Systems	Managed by a few private actors who share infrastructure governance. Participation is limited to members of the consortium.	Vodafone & Orange's Open RAN project in Europe.[10]
Permissioned Networks	Access is limited to approved actors.	Some government cloud systems or health data exchanges.[11]

8. Verburg and Lehman, "Overview of Telecommunications Telecommunication Policy and Governance."

9. Rios, "The Wolf of MWC."

10. O'Halloran, "Orange and Vodafone Work Together to Develop Open RAN Sharing in Rural Europe | Computer Weekly."

11. "First Sovereign Cloud Platform For The German Administration On The Home Straight - Bertelsmann SE & Co. KGaA."

Open Standards-Based Infrastructure	Built on transparent, publicly available standards enabling interoperability and modular development.	Estonia's X-Road.[12]
Multistake-holder Systems	Shared governance among the government, the private sector, and civil society with shared responsibilities in design and oversight.	Brazil's Internet Steering Committee (CGI.br).[13]
Permissionless Open Networks	Participation and contribution are open to any actor with varying degrees of prior approval.	Guifi.net in Spain.[14]
Decentralized Autonomous Networks	No central authority; governance and operation are distributed.	Emerging Web3 and blockchain-based infrastructures.

Key Insight

The most promising systems combine open standards, modular design, and multistakeholder governance without defaulting to either fully open or fully closed extremes.

The India Stack is a case in point: while the first wave of digital infrastructure solutions heavily relies on government-mandated identity and payments infrastructure, it has inspired a second generation of more open and distributed services with open API and open protocols like Beckn. Today, this hybrid model has enabled 8.6 billion mobile payments per month for 1.2 billion people – at minimal cost and maximum scale. However, the model is not without risks. The concentration of sensitive personal data within core systems means that breaches, when they occur, can have outsized consequences. Building openness must go hand in hand with strong data protection, redress mechanisms, and continuous security reinforcement.

Importantly, openness does not mean insecurity. Having multiple actors participating in a system actually enhances resilience and reduces the risks associated with centralized blind spots or single points of failure. Additionally, with the right protocols, transparency can enhance trust and resilience. Properly implemented, open standards and protocols can strengthen system resilience and public trust. Estonia's X-Road shows how open-by-design systems can scale securely. As digital infrastructure becomes the backbone of economies and, designing for openness, where appropriate, is not just a technical choice, but a state imperative.

Finally, policymakers do not need to choose between strictly open or closed infrastructure – these are false binaries. Instead, they must ask: Where do we need control, and where can openness enhance legitimacy, innovation, or trust? A modular, hybrid design, rooted in open standards and strong governance, offers the best of both worlds.

12. "X-Road – interoperability services."

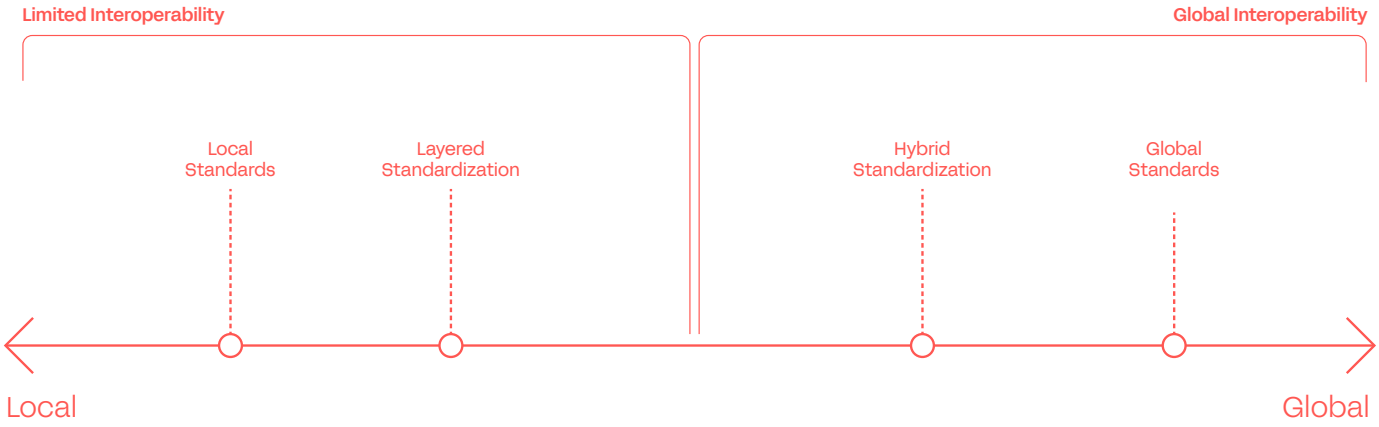
13. NIC.br, "CGI.br - Comitê Gestor da Internet no Brasil."

14. Dalmau, "What Is Guifi.Net?"

2.2 Scope: Global vs Local

The tradeoff between local and global systems is a critical consideration in designing infrastructure, standards, and governance models. Local systems offer customization, flexibility, and relevance to specific regions, while global systems provide scalability and interoperability, oftentimes at a lesser cost.

This is not a binary choice. The key question is: How can governments build locally relevant systems that also connect to global networks?



Comparison of Approaches

Approach	Description	Use Case Examples
Local Standards	Local standards are developed and implemented independently to reflect a country's specific needs, legal frameworks, technical capacity, and cultural values.	Early Aadhaar, national health records
Layered Standardization	This model uses international standards as a base but allows for tailored national or sector-specific adaptations.	ISO standards adapted regionally
Hybrid Standardization	Hybrid approaches give equal emphasis to global and local priorities. Standards are co-designed, often through inclusive, multi-actor engagements, to maximize both interoperability and contextual relevance.	OpenCRVS, national ID systems based on MOSIP

Global Standards	Complete adherence to international frameworks, ensuring interoperability and consistency but limiting local customization.	SWIFT, TCP/IP, W³C standards

Each spectrum of standardization choices offers distinct strengths and trade-offs. Local standards offer strong alignment with national priorities and control over data governance, making them ideal for sensitive sectors like health and identity—but they risk fragmentation and limited global interoperability. Layered standardization builds on international norms with tailored national adaptations, striking a balance between global compatibility and local relevance, especially useful in finance or trade. Hybrid models co-design standards through inclusive processes, maximizing interoperability and trust across borders, but often require complex governance and slower consensus. Global standards ensure seamless integration and operational consistency across borders—essential in areas like internet protocols or cloud services—yet can overlook local needs and disproportionately reflect the priorities of global actors. Smart policy design must weigh sovereignty, speed, and scalability to match sectoral demands.

Key Insight

There is strong sovereignty in chosen collaboration.[15] Being globally interoperable doesn't mean being globally dependent. For instance, the India Stack illustrates how a national digital infrastructure can be rooted in local legal and social needs, use open protocols to ensure interoperability, and support ecosystem-wide innovation (public and private actors). Its architecture, even though retrofitted since it wasn't designed to be globally interoperable in the first place, proves that strategic openness enables both sovereignty and scale.

The tradeoff between local and global standards is crucial in shaping effective digital infrastructure. While local standards offer tailored solutions with high relevance and control, they can hinder broader interoperability. Layered and hybrid standardization models provide flexible frameworks that balance global consistency with local needs, fostering collaboration without compromising region-specific solutions. Global standards, though ideal for cross-border operations, may not always address unique local contexts.

Ultimately, the goal is to strike the right balance between local sovereignty and global interoperability, ensuring that digital systems are both adaptable and resilient in a rapidly evolving, interconnected world. Interoperability does not have to mean uniformity and identical systems. Similarly, data localization does not mean data sovereignty. True sovereignty depends on how infrastructure is governed, by whom, and under what rules, not just where the servers sit. In this sense, this is less of a trade-off and more of a design challenge. Therefore, dependence on a few players for cloud infrastructure, or overcorrection by overreliance on private actors in Eurostack proposals must be considered carefully.

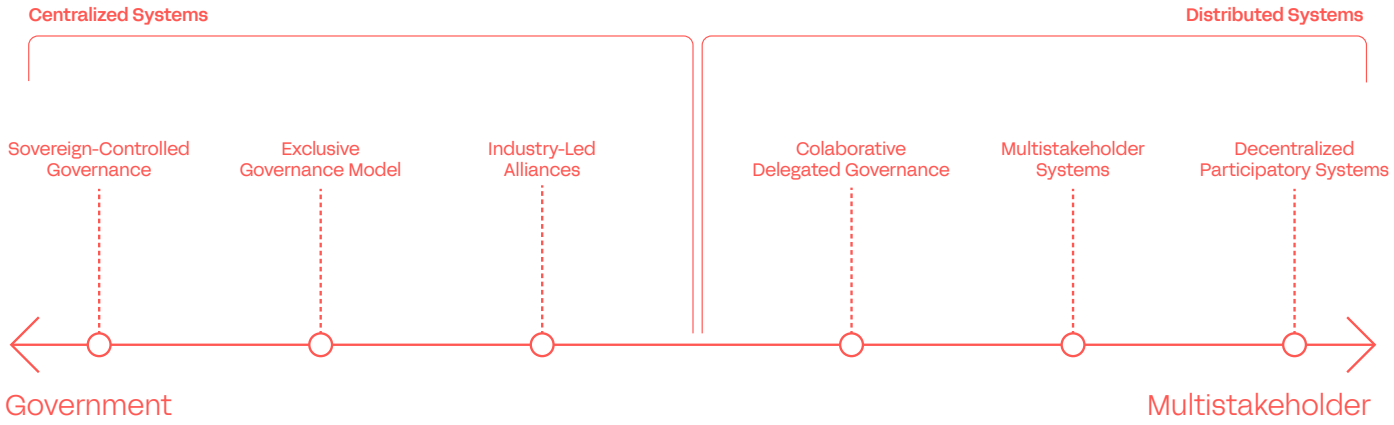
15. Berjon, "Digital Sovereignty."

2.3 Governance: Government vs Multistakeholder

The governance of digital infrastructure is a delicate balancing act, spanning a spectrum from centralized control (typically government-led) to distributed, multistakeholder collaboration. Each governance model brings unique strengths and challenges: centralized control can drive efficiency and ensure better coordination at the national level, but may lack inclusivity, while multistakeholder governance can foster broader collaboration but can struggle with coordination and direct accountability. Understanding where on this spectrum to position governance mechanisms is key to ensuring that digital infrastructure is not only secure and efficient, but also equitable, inclusive, and adaptable

Key Diagnostic Questions for Policymakers

Design Models	Questions
Governance Structure and Decision-Making	Who owns/drives the project? Which stakeholders – government, private sector, civil society, technical experts, academia – should be involved, and how are their inputs weighted? To what extent should governance be centralized, and when is distributed control more effective?
Stakeholder Roles and Sectoral Leadership	Where is public sector leadership essential, and where should the private sector take the lead? How do you prevent regulatory/political capture when you involve industry? Can governance models support agility and experimentation without compromising security, equity, or long-term vision? What mechanisms ensure that decision-making processes remain transparent, inclusive, and aligned with the public interest?



Comparison of Approaches

Approach	Description	Use Case Examples
Sovereign-Controlled Governance	A single national authority exercises full control, enabling rapid decision-making and policy cohesion, minimizing bureaucratic friction. It has limited inclusivity, low transparency, and reduced adaptability. Innovation can stall, trust may erode, and the system risks brittleness.	Aadhaar,[16] China's e-CNY
Exclusive Governance Model	Concentrates governance within a small group of trusted entities – usually government and select private partners – allowing tight control, strategic coherence, and streamlined decisions. Limited external input makes it harder to respond to changing needs and technologies. The result is stability, but often at the expense of adaptability.	Australia's NBN & Government Business Enterprise (GBE), Singpass
Industry-led Alliances	Private sector alliances steer infrastructure and operations, leveraging market agility for rapid innovation and deployment. This model excels in speed and adaptability. But without strong oversight, accountability weakens. Profit-driven decisions can sideline public interest, equity, and resilience. Efficiency often costs inclusivity and broader societal goals.	Stargate Project, Global Artificial Intelligence Infrastructure Investment Partnership (GAIIP), 5G Telecom consortiums
Collaborative Delegated Governance	Public and private actors share responsibility – combining state legitimacy with private sector agility. This enables inclusive, adaptable solutions in complex domains like digital strategies or cybersecurity. But diverging agendas, power imbalances, and bureaucracy can stall progress. Without strong alignment and accountability, collaboration risks fragmentation.	Canada's DIACC

16. Yadav, "Digital Exclusion: Poor, Elderly Face the Brunt of Aadhaar-Based Authentication Errors."Yadav, "Digital Exclusion."

Multistakeholder Systems	It brings together government, industry, civil society, academics etc. to co-shape decisions, emphasizing inclusivity, transparency, and shared accountability. But coordination can be complex, consensus slow, and enforcement weak—especially when interests clash or urgency demands speed. Without strong facilitation and clear processes, it risks being more aspirational than effective.	ICANN, CGI.br
Decentralized Participatory Systems	Governance operates without a central authority, relying on a decentralized network of stakeholders. It maximizes inclusivity, resilience, and grassroots innovation, but can lack coordination. Decision-making can become fragmented, enforcement inconsistent, and accountability diffused. Without conflict resolution or alignment, the system risks inefficiency and gridlock. Distributed models require high trust and coordination to scale effectively.	Guifi.net

Key Insight

It is key to understand that technical choices, while important, are not sufficient on their own. Without governance models supporting and reinforcing them, even the most well-designed technical infrastructures can fall short of their intended impact. For example, an open digital infrastructure does not guarantee open or inclusive governance. Digital commons risk being undermined when governance structures do not reflect or advance the values embedded in their technical design. Aligning technical choices with governance choices is fundamental.

The best governance model often blends aspects of the models discussed above. Drawing inspiration from internet governance structures, particularly non-profit, open participation frameworks, can offer a balanced solution. These models prioritize transparency, accountability, and broad stakeholder involvement while ensuring that decisions are made in the public interest.

Taking inspiration from the internet governance models, particularly the Internet Corporation for Assigned Names and Numbers (ICANN) model, might certainly prove helpful. Governments should explore governance mechanisms that combine the strengths of centralized oversight and focused decision-making with the agility and innovation of the private sector and inclusivity offered by multistakeholder collaboration resulting in shared accountability reinforcing trust and legitimacy. By doing so, they can create resilient and responsive governance structures capable of adapting to rapidly evolving digital landscapes.

Step 3: Safeguarding

As governments and societies grapple with the challenge of governing digital infrastructure for public good, each model – from sovereign centralized control to decentralized participation – brings trade-offs that must be carefully managed through smart, context-sensitive safeguards. A forward-looking governance strategy requires regulatory agility, accountability, and a firm grounding in public interest.

Government oversight alone is not a safeguard. In some contexts, it can become a source of harm, enabling censorship, exclusion, or abuse. That's why strong civil society participation and multistakeholder governance are vital. They don't just hold power to account; they help build a digital future defined by transparency, inclusion, and the public interest.

Therefore, across governance models, regardless of how centralized or decentralized they are, there is a set of basic minimum safeguards that are non-negotiable if the goal is to build trust, usefulness, and responsiveness into digital infrastructure. These cross-cutting safeguards ensure that no matter who governs, the public interest remains front and center:

Safeguards	Description
Transparency by Design	Mandatory disclosure of decision-making processes, governance structures, and performance metrics. Example: Public registers for contracts, standards, and data-sharing agreements.
Accountability Mechanisms	Independent oversight bodies or ombuds institutions. Clear lines of responsibility, redress mechanisms, and enforcement authority. Example: Regulatory levers to prevent monopolistic infrastructure control.
Public Interest Impact Assessments	Regular evaluations to assess how infrastructure decisions affect equity, privacy, competition, and access. Example: Requirement to publish and respond to these assessments.
Inclusive Stakeholder Engagement	Structured mechanisms for meaningful consultation (not just token input) from civil society, local communities, and underrepresented groups. Example: Minimum stakeholder representation quotas in governance boards or advisory groups.

Rights-Based Frameworks	Embedding fundamental digital rights (privacy, non-discrimination, access, due process) into governance charters and legal instruments. Adherence to international human rights norms. Example: connecting the UN's Global Digital Compact (GDC) to local contexts.
Data Governance Safeguards	Clear rules on data ownership, access, and use – particularly in shared or decentralized systems. Example: Requirements for data minimization, portability, and fiduciary responsibilities.
Resilience and Continuity Planning	Safeguards for infrastructure continuity in the face of political shifts, cyber threats, or governance breakdown. Example: Through scenario planning and regular stress-testing.
Sunset Clauses and Periodic Review	Built-in mechanisms for revisiting governance structures, especially during rapid technological change. Example: Expiration or renewal clauses tied to performance and public interest outcomes.
Whistleblower Protections and Civic Tech Participation	Safe channels for exposing governance failures. Support for civic tech and public audit tools that enable bottom-up accountability.

These safeguards serve as the baseline safeguards necessary to protect against capture, corruption, and collapse – no matter where on the spectrum a model sits. They do not dictate a specific governance form but ensure all forms serve democratic, equitable, and future-ready goals.

The UN's Global Digital Compact– adopted by all UN member states– already provides a broad umbrella of globally agreed-upon commitments to embedding privacy and data agency in digital infrastructure, but these need to be operationalised through more granular action plans. Multilateral fora like the G7 and the G20 and international organizations like the United Nations (UN), International Telecommunication Union (ITU), and the Organisation for Economic Co-operation and Development (OECD) play a crucial role in developing and upholding global norms and minimum standards - especially in domains where risks and opportunities are inherently international. This is already being done as evidenced by the successful and continued global dialogue on the Hiroshima AI Principles by the G7, and the formation of a new Task Force on AI and Data Governance by the G20. These groups could help fcross-border regulatory coherence—especially in areas like platform accountability, and biometric data; and strengthen oversight capacity (help countries build institutions—data protection authorities, ethics councils, audit regimes) and influence funding and procurement guidelines.

Step 4: Adopting

The success of a digital economy hinges not only on building robust infrastructure but also on empowering citizens to engage with and benefit from these systems. As highlighted, multistakeholder engagement is essential at every stage for the widespread adoption of digital infrastructure. Trust, usefulness, and responsiveness are the core principles that drive this adoption.

When digital systems fail, it is often due to a lack of user-centered design or a failure to incorporate citizen feedback. Digital citizens, as the end-users, must be engaged throughout the process – not just as passive recipients but as active participants in the design and evaluation of digital services. For instance, the India Stack, while transformative, illustrates this gap: of the 540.3 million accounts opened under the Pradhan Mantri Jan Dhan Yojana (PMJDY), 113 million remain inoperative.[17] This underscores the risks of designing at scale without grounding systems in real user needs, behaviours, and feedback. Frequent feedback loops are crucial for identifying flaws, enhancing inclusivity, and fostering trust in digital systems. Many governments' initiatives such as surveys and participatory frameworks developments have proven benefits from including citizens such as the Taiwanese platform join.gov.tw or the Canadian DIACC collaboration with the platform PlaceSpeak for online consultations. However, to participate meaningfully, citizens need to have a foundational understanding of their digital lives and the value of their data.

4.1 Unlocking Digital Literacy

Overall, while citizens have very limited understanding of their digital selves, their data, privacy online and why concretely this all matters,[18] they show clear concerns and distrust over their personal data collection.[19]

The cycle of underutilization presents a "chicken-and-egg" problem. People are not aware of resources because they lack knowledge of how to engage with them, and because of this, the demand for alternative, user-centric digital services is not strong enough to drive innovation. "Without ease of use" and "ease of adoption" – potential adopters will be hamstrung without accessible guidance on how to implement and socialize the infrastructure/standards. Governments can break this cycle by actively promoting data agency tools, hosting digital literacy physical workshops or online mooc, and ensuring that citizens have easy access to educational resources about their rights and responsibilities in the digital space.

17. "About 20% of 510 Mn Jan Dhan Accounts Inoperative."

18. "56% of EU People Have Basic Digital Skills."

19. Bell and Theodule, "Report IV: People Want Control of Their Data."

At the very foundational level, governments have a responsibility to ensure digital literacy. Governments must invest in digital literacy initiatives that go beyond basic technical skills to focus on the meaning and management of digital identities. For instance, Singapore's Smart Nation initiative focuses on equipping citizens with digital literacy skills, including knowledge on managing their digital identities safely. Moreover, part of the digital infrastructure development "Kenya National Digital Masterplan" covering the decade 2022-2032, is a massive digital literacy capacity-building initiative targeting 20 million citizens, 10,000 ICT professionals with advanced skills, 300,000 public servants, and 350,000 teachers.

4.2 Campaign on the Value of Data

Next, citizens must understand their data's multi-faceted value and their rights over it. Without a basic understanding of why and what data is being collected, how it is used, and what rights individuals have over it, people cannot fully leverage their digital identities as assets. Governments have the responsibility to launch public awareness campaigns aimed at educating citizens about the economic and social value of their data. This includes explaining how their digital identities contribute to innovation, personalized services, and even economic growth. By showing people that their data is a crucial part of their digital DNA, governments can inspire them to take ownership and responsibility for it. For example, the UK's "Your Data Matters" campaign helped people understand how their personal data drives services like healthcare apps, online shopping, and entertainment.

At the same time, it is a reasonable assumption not every individual will be an expert on data – in this context, the use cases of trusted data intermediaries, data cooperatives, data spaces and other such mechanisms must be continuously explored and improved. For example, a range of "data collectives" – from trusts to cooperatives to commons – are developing various governance mechanisms allowing end users to pool and leverage their data resources for the public good. Also a nascent but growing sector of "Net fiduciaries," such as Consumer Reports, aims to provide a wide array of digital services to their clients and customers under common law-derived duties of care and loyalty. The proliferation of compelling use cases by all these trust-based entities will enhance digital literacy and the understanding of one's data value which will ultimately allow better protection of users' data.

Conclusion

The decisions governments make today regarding digital infrastructure will profoundly shape the trajectory of their societies, economies, and citizens' lives for decades to come. This Toolkit emphasizes that the future need not be left to chance or dominated by narrow interests. Instead, by adopting a holistic and strategic approach, anchored in principles of trust, usefulness and responsiveness, governments can confidently navigate complex trade-offs and unlock digital ecosystems that are resilient, inclusive, and adaptable. Embracing this proactive role will allow governments not only to reclaim their space as effective shapers of technological progress but also to foster an environment where innovation aligns with public interest.

Achieving this vision demands sustained commitment, collaboration, and oversight. It requires active dialogue with civil society, responsible engagement with private sector innovators, and meaningful cross-border cooperation. This toolkit is not meant as a comprehensive and finished guidance, it lays the foundation for sustained and practical engagement. It calls for continual reassessment and responsiveness, recognizing that technological contexts and societal expectations will inevitably evolve.

By embedding transparency, accountability, and data agency as foundational principles rather than afterthoughts, governments can ensure the infrastructure they build today remains trustworthy, useful, and secure. Ultimately, this is more than a technological endeavor; it is a commitment to strengthening governance, empowering citizens, and cultivating a digital landscape that reflects and serves the needs of all members of society, both now and in the future.

While this Toolkit sets out a strategic vision and foundational approach, it acknowledges that questions of financing and long-term sustainability of digital infrastructure require deeper exploration. Building on the recommendations of the Fair Data Economy Task Force, our next steps will focus on conducting a comprehensive economic impact study to better understand the value, costs, and returns of public-interest digital infrastructure. This work will serve as the basis for forging major infrastructure investment alliances and for establishing a Global Public-Private Digital Infrastructure Hub—an initiative aimed at aligning resources, knowledge, and capacity at scale. In parallel, we will begin shaping a practical roadmap to help bridge institutional silos across government ministries and agencies, enabling more coordinated, coherent, and impactful digital infrastructure strategies implementations. In doing so, we aim to ensure that the ambition outlined here is matched by the means to realize it, paving the way for resilient, inclusive, and future-ready digital foundations.

Bibliography

"56% of EU People Have Basic Digital Skills," December 15, 2023. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/DDN-20231215-3.

Abate, Carolina, Giuseppe Bianco, and Francesca Casalini. "Concurrence dans la chaîne d'approvisionnement alimentaire." OCDE, January 16, 2025. https://www.oecd.org/fr/publications/concurrence-dans-la-chaine-d-approvisionnement-alimentaire_eeeab061-fr.html.

"About 20% of 510 Mn Jan Dhan Accounts Inoperative: MoS Finance Informs RS," December 19, 2023. https://www.business-standard.com/india-news/about-20-of-510-mn-jan-dhan-accounts-inoperative-mos-finance-informs-rs-123121901001_1.html.

Airan, Avani. "Landscaping Infrastructures for the Digital Ecosystem | TechPolicy.Press." Tech Policy Press, November 8, 2024. https://techpolicy.press/landscaping-infrastructures-for-the-digital-ecosystem.

Apolitical. "How Estonia Fights Covid-19 by Going Online," 2020. https://apolitical.co/solution-articles/en/estonia-fights-covid-19-by-going-online.

Atlantic Council. "What Should Digital Public Infrastructure Look like? The G7 and G20 Offer Contrasting Visions," April 18, 2024. https://www.atlanticcouncil.org/blogs/new-atlanticist/what-should-digital-public-infrastructure-look-like-g7-g20/.

Bartley, Rachel. "The Economics of Shared Digital Infrastructures | Bartlett Faculty of the Built Environment," March 31, 2025. https://www.ucl.ac.uk/bartlett/publications/2025/mar/economics-shared-digital-infrastructures.

Bell, Jeb and Jessica Theodule. "'Globally, People Want Control of Their Data.'" Project Liberty Institute, 2024. https://www.projectliberty.io/wp-content/uploads/2024/12/PL_Insights_Report-IV-1.pdf.

Berjon, Robin. "The Fiduciary Duties of User Agents." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, April 15, 2021. https://doi.org/10.2139/ssrn.3827421.

Bradford, Anu. "Digital Empires: The Global Battle to Regulate Technology." Oxford, New York: Oxford University Press., 2023. https://academic.oup.com/book/46736#.

Bria, Francesca. "The Quest for European Technological Sovereignty: Building the EuroStack | TechPolicy.Press." Tech Policy Press, October 15, 2024. https://techpolicy.press/the-quest-for-european-technological-sovereignty-building-the-eurostack.

Bria, Francesca, Paul Timmers, and Fausto Gernone. "EuroStack – A European Alternative for Digital Sovereignty," 2025, 127 p. https://doi.org/10.11586/2025006.

Charlotte Hess and Elinor Ostrom. "Understanding Knowledge as a CommonsFrom Theory to Practice | Books Gateway | MIT Press," 2006. https://direct.mit.edu/books/edited-volume/3807/Understanding-Knowledge-as-a-CommonsFrom-Theory-to.

"Cloud AI Market Size | Mordor Intelligence." Accessed April 15, 2025. https://www.mordorintelligence.com/industry-reports/cloud-ai-market.

"Redefining Infrastructure in the Digital Age: The Rise of Digital Public Infrastructures." Reframe[Tech] (blog), October 23, 2024. https://www.reframetech.de/en/2024/10/23/redefining-infrastructure-in-the-digital-age-the-rise-of-digital-public-infrastructures/.

Dalmau, lluis. "What Is Guifi.Net?," 2009. https://guifi.net/node/22157.

"Data Protection Day: Only 1.3% of Cases before EU DPAs Result in a Fine." Accessed April 15, 2025. https://noyb.eu/en/data-protection-day-only-13-cases-eu-dpas-result-fine.

Degeling, Martin, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. "We Value Your Privacy ... Now Take Some Cookies." Informatik Spektrum 42, no. 5 (October 1, 2019): 345–46. https://doi.org/10.1007/s00287-019-01201-1.

e-Estonia. "X-Road – interoperability services," June 10, 2024. https://e-estonia.com/solutions/x-road-interoperability-services/x-road/.

Fehlinger, Paul, Jeb Bell, Claire McBride, and Maria Farrell. "'Toward a Fair Data Economy: A Blueprint for Innovation and Growth.'" Project Liberty Institute, 2024. https://www.projectliberty.io/wp-content/uploads/2024/11/Project-Liberty-Institute-Toward-a-Fair-Data-Economy-A-Blueprint-for-Innovation-and-Growth-Action-Recommendations-of-the-Project-Liberty-Fair-Data-Economy-Task-Force.pdf.

"First Sovereign Cloud Platform For The German Administration On The Home Straight - Bertelsmann SE & Co. KGaA." Bertelsmann SE & Co. KGaA, Carl-Bertelsmann-Straße 270, D-33311 Gütersloh, www.bertelsmann.com, 2024. https://www.bertelsmann.com/news-and-media/news/first-sovereign-cloud-platform-for-the-german-administration-on-the-home-straight.jsp.

Ford, Camille, Marta Dell'Aquila, Olesya Grabova, and Andrea Renda. "CEPS IN-DEPTH ANALYSIS," March 2025.

Francescomacri, Di. "Towards the G7 Summit: T7 Italy Communiqué." RIFLESSIONI (blog), June 5, 2024. https://francescomacri.wordpress.com/2024/06/05/towards-the-g7-summit-t7-italy-communique/.

Hung, Kai-Hsin. "Beyond Big Tech Geopolitics | Transnational Institute," March 29, 2025. https://www.tni.org/en/article/beyond-big-tech-geopolitics.

Kaltheneuer, Frederike, Leevi Saari, Amba Kak, and Sarah Myers West. "'Redirecting Europe's AI Industrial Policy: From Competitiveness to Public Interest.,'" 2024. https://ainowinstitute.org/wp-content/uploads/2024/10/AI-Now_EU-AI-Industrial-Policy_Oct.-2024.pdf.

Kapur, Akash. "From Digital Sovereignty to Digital Agency." New America, 2024. http://newamerica.org/planetary-politics/briefs/from-digital-sovereignty-to-digital-agency/.

Katja, Bego. “Towards Public Digital Infrastructure: A Proposed Governance Model.” nesta, 2022. https://www.nesta.org.uk/project-updates/towards-public-digital-infrastructure-a-proposed-governance-model/.

Komaitis, Konstantinos. “Analysis: A Brave New Reality after the UN’s Global Digital Compact.” DFRLab (blog), October 1, 2024. https://dfrlab.org/2024/10/01/analysis-a-brave-new-reality-after-the-uns-global-digital-compact/.

“Internet Fragmentation: Why It Matters for Europe:: EU Cyber Direct.” Horizon, January 31, 2023. https://eucyberdirect.eu/research/internet-fragmentation-why-it-matters-for-europe?utm_source=chatgpt.com.

Krewer, Jan. “Investing in Public Digital Infrastructure.” Open Future, 2024. https://openfuture.eu/publication/investing-in-public-digital-infrastructure.

Krewer, Jan. “Looking for an Exit: Europe’s Way to Public Digital Infrastructures | TechPolicy.Press,” March 2025. https://www.techpolicy.press/looking-for-an-exit-europes-way-to-public-digital-infrastructures/.

Media. “DECODE – Decentralised Citizens Owned Data Ecosystem (EU Project).” Nexa Center for Internet & Society (blog), December 22, 2016. https://nexa.polito.it/decode/.

Metagov Seminar - Digital Public Infrastructure to Unlock Each Person’s Economic Potential (Rowan), 2025. https://www.youtube.com/watch?v=wxdCVXan7u0.

Mozur, Paul, and Adam Satariano. “Russia, in New Push, Increasingly Disrupts Ukraine’s Starlink Service.” The New York Times, May 24, 2024, sec. Technology. https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html.

NIC.br. “CGI.br - Comitê Gestor da Internet no Brasil.” CGI.br - Comitê Gestor da Internet no Brasil. Accessed April 15, 2025. https://cgi.br.

Nicole, Sarah, Jeb Bell, Christian Kastrop, Vidisha Mishra, Paul Fehlinger, and Mateo Rodriguez. “Digital Infrastructure Solutions to Advance Data Agency in the Age of Artificial Intelligence.” Project Liberty Institute, December 2024. https://www.projectliberty.io/news/advancing-data-agency/.

O’Halloran, Joe. “Orange and Vodafone Work Together to Develop Open RAN Sharing in Rural Europe | Computer Weekly.” ComputerWeekly.com, 2023. https://www.computerweekly.com/news/365531410/Orange-Vodafone-team-to-develop-Open-RAN-sharing-in-rural-Europe.

“Revolutionizing Digital Commerce: The ONDC Initiative,” 2025. https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=2090097.

Rios, Danielle. “The Wolf of MWC.” TelcoDR, March 11, 2025. https://telcodr.com/insights/starlink-telco-partnerships-blog/.

Robin Berjon. “Digital Sovereignty,” February 25, 2025. https://berjon.com/digital-sovereignty/.

Robin Berjon. “The Public Interest Internet,” June 17, 2024. https://berjon.com/public-interest-internet/.

Schrepel, Thibault. “Ela Głowicka & Jan Málek: ‘Digital Empires Reinforced? Generative AI Value Chain.’” Network Law Review (blog), March 18, 2024. https://www.networklawreview.org/glowicka-malek-generative-ai/.

Shalal, Andrea, and Joey Roulette. “Exclusive: US Could Cut Ukraine’s Access to Starlink Internet Services over Minerals, Say Sources.” Reuters, February 22, 2025, sec. Business. https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/.

Snower, Dennis and Paul Twomey. “‘Empowering Digital Citizens Report.’” The Global Solutions Initiative and the Global Initiative for Digital Empowerment (GIDE)., 2022. https://www.global-solutions-initiative.org/programs/digital-empowerment/empowering-digital-citizens-report/.

Soni, Shivam, and Admin Aapti. “Aapti Institute | The Governance of Digital Public Infrastructure.” Aapti Institute, June 15, 2024. https://aapti.in/blog/the-governance-of-digital-public-infrastructure/.

Soujanya, Sridharan, Vinay Narayan, Jack Hardinges. “Digital Public Infrastructure: Orientation Matters.” Centre for International Governance Innovation. Accessed April 15, 2025. https://www.cigionline.org/articles/digital-public-infrastructure-orientation-matters/.

Statista. “Global Cloud Infrastructure Market Share 2024.” Accessed April 15, 2025. https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/

The Open Data Institute. “ODI and Solid: Building a Future Where Data Works for Everyone,” October 17, 2024. https://theodi.org/insights/projects/odi-and-solid-building-a-future-where-data-works-for-everyone/.

The Open Data Institute. “The Data Spectrum.” September 26, 2020. https://theodi.org/insights/tools/the-data-spectrum/.

Verburg, Gary, and Laura Lehman. “Overview of Telecommunications Telecommunication Policy and Governance,” 2016. https://www.columbia.edu/itc/sipa/nelson/ict4cuba-export/mainSpace/Overview%20of%20Telecommunication.html.

Whitt, Richard, Reweaving the Web. The Book SHelf Ltd., 2024. https://www.reweavingtheweb.net/.

“‘X-Road Factsheet.,’” 2024. https://e-estonia.com/wp-content/uploads/factsheet_x-road.pdf.

Yadav, Anumeha. “Digital Exclusion: Poor, Elderly Face the Brunt of Aadhaar-Based Authentication Errors.” The Wire, 2024. https://thewire.in/rights/digital-exclusion-poor-elderly-face-the-brunt-of-aadhaar-based-authentication-errors.

Defining Key Concepts: Core and Relevant Terms for This Report

Disclaimer: The terms below are our operative definitions to limit the scope of this multistakeholder and research initiative. They are extensively explained throughout the text.

Core Terms in Our Framework

// Data Agency: The ability of citizens to have control over their personal data, including how it is used, shared and monetized, ensuring they have true voice, choice and stake.

// Fair Data Economy: An economic model where citizens have control over their data, platforms are interoperable, and value is equitably distributed, fostering innovation and sustainable growth.

// Digital Infrastructure Solutions: refer to the foundational physical and technical systems, at the critical intersection where physical infrastructure meets public governance. These solutions determine how data is transmitted, stored, and processed, and shape access, control, and power dynamics across the digital ecosystem. They exclude application-level features and focus instead on the core systems that enable digital connectivity and services. They encompass but are not limited to broadband networks, advanced data architectures, and next generation protocols and standards etc. This concept is central to driving our work.

// Toolkit: This toolkit is not meant to be comprehensive, nor does it claim to offer one-size-fits-all answers. Instead, it is designed as a practical and engaging starting point for policymakers, public officials, and institutional leaders who are looking to deliberate, co-create, and design digital infrastructure solutions that serve the public interest. It includes a curated set of questions and examples to equip decision-makers with enough clarity to ask better questions, make informed trade-offs, and foster collaboration across sectors—rather than prescribing fixed solutions.

Relevant Terms Outside Our Framework

// Data Sovereignty: Principle that data is subject to the laws and governance of the state in which it is collected. It reflects a state's right to control data flows and content dissemination within its borders. This term is also used in the context of cultural heritage e.g. data sovereignty of Indigenous communities - although this aspect has not been covered within this report.

// Digital Public Infrastructure: There are multiple, often competing definitions of this concept, with no globally agreed-upon framework, as discussed in our **intermediary report**.