C4AIE Digital Technologies

WORLD ECONOMIC FORUM

State of Play: Preparedness for the Connected Future

JULY 2025

Introduction

Remaining competitive and agile in any industry or sector requires scalable and future-ready digital capabilities to facilitate the development and delivery of products and services. Digital public infrastructure (DPI) – including elements such as digital identity, data processing and exchange, and digital ownership – provides a foundation upon which these capabilities can be developed, scaled and innovated.

While maintaining DPI systems is often a public sector project, innovation and new system development are largely driven by the private sector, fueled by commercial and consumer demand for emerging technologies such as artificial intelligence (AI), extended reality (XR) and biometrics in an advancing digital landscape. Trustworthiness, interoperability and utility of next-generation products and services built on DPI must be continually evaluated, but prioritizing DPI development is essential to enable the economic and societal benefits of emerging technologies.

DPI must be effectively developed and responsibly adopted so that the future of digital interchange, including the agentic web, can be delivered at scale and remains open, accessible and democratic, with sustainable infrastructure for communication, commercial activity and societal interaction.

Data exchange and processing

At the most foundational level of the digital tech stack is the physical infrastructure that powers, scales and drives processing for all downstream services. Since its inception, the internet's physical infrastructure has grown into a vast, layered system designed to support global connectivity and data exchange. At its core are transoceanic subsea cables, which currently carry 95% of international data.[1]

On land, terrestrial fiber networks connect cities and regions, feeding into data centres that process, store and route vast volumes of information. These data centres – ranging from small server rooms to massive hyperscale facilities – have historically been built for general-purpose computing, with standard air cooling and modest power densities. Wireless towers, local exchanges and undersea landing stations have also extended the internet's reach, enabling broadband, mobile data and cloud services to scale globally.

Traditionally, infrastructure development was shaped by the needs of web hosting, video streaming, cloud storage and enterprise computing, all of which drove incremental advances in speed, capacity and geographic coverage. Today, however, the physical infrastructure supporting digital services is rapidly evolving to meet the demands of AI, which requires significantly more compute power, electrical capacity and low-latency data delivery than traditional web services. McKinsey estimates that demand for data centre capacity will increase by ~20% per year from 2023-2030.[2]

To meet this demand, data centre design and construction must address how to scale with higher efficiency and lower environmental impact. Alongside these, global subsea cable networks remain the backbone of international data transfer, now being upgraded for higher bandwidth and improved resilience to accommodate AI-driven traffic surges. Low Earth orbit (LEO) satellites are emerging as critical complements, extending internet access to remote regions and enabling faster, more reliable connections for real-time AI applications. Together with terrestrial fiber networks and edge computing nodes, these components form a more distributed, energy-aware and latency-optimized architecture that reflects the growing centrality of AI in global digital infrastructure.

Forecast

Recent global events have highlighted the vulnerabilities of the internet's physical infrastructure in two key areas. First, data centres are facing increased energy and performance demands by the scaling of AI and XR, exacerbated by mechanical overcrowding, inefficient cooling and outdated hardware. This demand can be answered with more design-efficient approaches and technology adoption, aided by public oversight, development support, monitoring and guidance on good practices. Data centres should consider the need for real-time data synchronization, spatial data privacy and contextual integrity safeguards, and interoperability standards for cross-platform data processing. Without these, as well as more distributed forms of hardware that support edge computing, scaling emerging technologies such as XR and AI will be severely limited.

The second area of vulnerability is situational and more volatile. Physical infrastructure, such as data centres, towers, or subsea internet cables, is critical infrastructure, facilitating the delivery of essential services and information delivery in times of crisis, emergency and war. Investment in the development and deployment of next-generation solutions such as LEO satellites can enable connectivity and continuity of essential operations amid traditional hazards. While this is an ongoing challenge dependent on geopolitical realities, public-private cooperation to ensure resilient physical infrastructure is essential to a robust future internet.

Data processing is also likely to be crucial to the further development of the agentic web, where AI agents are required to process data and make decisions or perform tasks on behalf of users. From acutely important use cases such as early medical detection and health optimization to everyday quality-of-life improvements like better recommendation systems, AI systems and agents will be a driving force in upleveling the internet. Their operations, though, must be tempered by clear and user-serving data transfer protocols, data processing norms and data inference practices. If these points are worked out and AI agents are designed in accordance with them, they can deliver on their positive impact while minimizing potential harms.

Digital identity

Digital identity is a layered and varied amalgamation of personalized data and identifiers that form unique profiles, enabling deeper personal utility, more robust security, and seamless movement across digital and blended spaces. The thinning categorical distinction separating traditionally conceptualized digital ID and digital identity is rapidly disappearing, making way for a more singular iteration, both essential to and for DPI.

This evolution is driven by two distinct yet uniquely intersecting trends, which are rapidly advancing the next generation of digital identity. The first trend comes as governments work to drive digital transformation, a process for which digital identity stands as the gateway to access a broad array of essential financial, healthcare, civic and educational services traditionally delivered offline. Effective architecture for digital identity has been made possible through close private-public partnerships focused on delivering services that are publicly offered, hosted and governed, but underpinned by private technology solutions.

In the United States, for example, the government's Internal Revenue Service offers online data retrieval and filing services that require identity verification protocols, provided by the private sector.[3] Similarly, Estonia's highly-regarded and advanced e-ID is underpinned by various private national companies facilitating authentication, verification and encryption protocols for seamless navigation and exchanges.[4]

The second trend is an expansion of technologies enabling digital identity and the data types that constitute it. These technologies broadly support the building and sustaining of a fluid digital identity, incorporating elements such as biometrics, physical health and body-based data, and secure service-interoperable profiles. These also serve to support traditional use cases such as security and credentialing.

The most ubiquitous form of expanded identity-related technologies is wearables and hardware that capture a repository of new classes of body-based user data, contributing to the building of a dynamic and multilayered digital identity. Fitbit or the Apple Watch, for example, capture significant amounts of personal data, including heart rate, sleep patterns and blood oxygen levels, which can be used – with appropriate user notice and consent – by both private and public entities, enabling use cases such as more affordable access to individualized health and wellness plans.[5]

Simultaneously, companies like CLEAR that capture biometric data[6] are expanding their business model from airport convenience to verification in additional venues such as stadiums and, more recently, as a safety mechanism through a partnership with Uber.

Both these trends are poised to continue offering tech solutions and services that enhance consumer experience while maximizing benefits. The risks that emerge, however, have little to do with the technology itself, but rather, how it is deployed and governed, particularly when multiple actors engage in multi-step data transactions with a wide user base, such as a nation's citizenry.

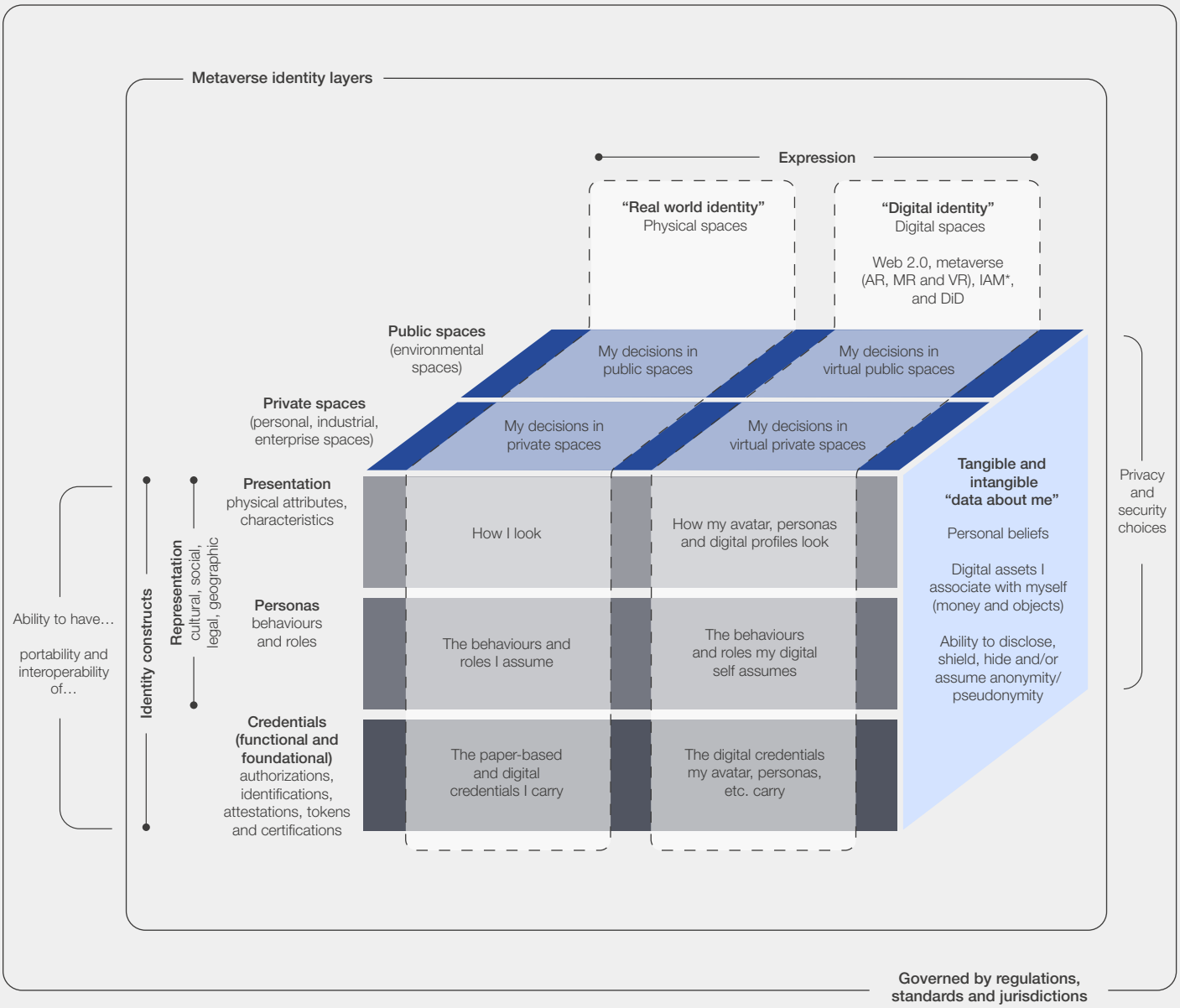
Forecast

The emerging challenge facing further development of DPI-supported digital identity will be primarily around interoperability, privacy and responsible data stewardship, particularly in the face of hardware designed for XR and AI-supported predictive capabilities.

Those capabilities, if responsibly delivered, offer massive value potential to users. For example, Ray-Ban Meta glasses offer a hands-free form factor and Meta AI integrations, allowing for new modalities of interaction and enabling physically disabled users new opportunities for access and utility.[7] Customizable AI agents, like those being developed by Meta, Google and OpenAI, can be informed by multimodal context and learn how to engage with a unique user. Digital identities will not only enable security, but also access to and value from technologies such as AI agents and smart wearables.

The concept of the agentic web also implies a need to fundamentally reassess how to understand digital identity and agency. Users have traditionally acted as their own agents, managing digital identities and their associated interactions. AI agents now operate on their behalf, extending digital identity while also performing independent, non-human tasks.[8]

Developing the agentic web in a safe, trustworthy way will require first understanding where and how digital identities square with agents, including on such topics as permission and consent, authentication and agent-to-agent interactions. Digital identity should be interoperable and must be constituted and utilized with user consent and ethical practices in the highest regard. The future internet, layered with XR and powered by AI, cannot exist without a continuous and interoperable digital identity that allows secure and uninterrupted user experiences.



*Identity and access management
**Decentralized identifiers

Digital wallets and ownership

Digital wallets and payment systems have been massively impactful as engines of economic growth and participation. Examples like Kenya's M-PESA, which launched in 2007 as a microfinance repayment platform and quickly grew to a full-service mobile payment system processing 56% of Kenya's GDP in 2023,[9] or India's Unified Payments Interface (UPI), an open-source digital wallet tool and protocol that has spread to hundreds of millions of users across at least seven countries,[10] showcase digital wallets' potential for impact in digital and financial inclusion.

But their utility is not limited to developing markets. As of 2025, nearly half of global consumers use digital wallets for bill payments, with significant usage in both online and in-store transactions.[11] In the US, 65% of adults reported using a digital wallet at least once in the past month,[12] and projections indicate global transaction value in excess of $17 trillion by 2029.[13]

While digital wallets are critical tools, growing their utility requires addressing interoperability, regulatory inconsistency – particularly in cross-border payment scenarios – user trust, and consistent and reliable network accessibility.

Forecast

The traction of multistakeholder programmes like the OpenWallet Foundation, a cooperation between the United Nations International Telecommunications Union and the Linux Foundation,[14] highlights digital wallets as a major driver of the internet's potential for even greater economic impact. As digital wallets evolve to store not only currency but also verifiable credentials and digital proofs, there is a growing need to ensure they are designed with interoperability and accessibility in mind. Ensuring broad access and seamless functionality across systems and borders is essential to unlocking their full societal

and economic potential. This will require interoperability and integration with legacy systems, open source, or common design standards to enable local deployment, and low bandwidth capabilities to ensure accessibility in low broadband areas.

DPI innovation and the future internet

The current internet's evolution to an agentic web promises a layered and enhanced experience driven by the transformative capabilities of emerging technologies. AI agents and AI-driven systems enhance creative capacity and productivity; XR and spatial computing redefine collaboration and communication; digital wallets and user-controlled portable data profiles advance interoperability.

As this unprecedented pace of digital innovation continues, the systems and infrastructure that support it must evolve in kind. Development across digital identity, data processing and digital ownership is essential to enable a move away from a stationary internet towards a dynamic digital experience.

As DPI evolves, stakeholders must take care to see it not for the sum of its parts, but rather for its overarching potential to support digital transformation and continued innovation – integrating future-friendly technologies into adaptable, user-friendly systems through global collaboration.

Contributors

World Economic Forum

Daniel Dobrygowski
Head of Governance and Trust

Dylan Reim
Connected Future Initiative Lead

Judith Vega
Connected Future Initiative Specialist

The Connected Future Working Group

This insight report is a combined effort based on numerous interviews, discussions, workshops and research. The opinions expressed herein do not necessarily reflect the views of the individuals or organizations involved in the project listed below. Sincere appreciation is extended to the following working group members, who spent numerous hours providing critical input and feedback on the drafts. Their diverse insights are fundamental to the success of this work.

Frank Badalamenti
Partner, PwC

Mahmoud Badawi
Assistant Minister for Digital Transformation, Ministry of Communications and Information Technology of Egypt

Andrew Barnhill
Chief Government Affairs Officer, IQVIA

Tony Burkart
Global Head, Workforce Development, Google Data Centers, Alphabet

Jordan Burris
Head of Public Sector, Socure

Jordan Fieulleteau
Head of Global Strategy, Reality Labs Policy, Meta Platforms

Daniel Goldsheider
Founder and Executive Director, OpenWallet Foundation

Craig Hamill
Director, Innovation & Technology Underwriters Laboratories

Brittan Heller
Fellow, Digital Forensics Research Lab, The Atlantic Council

Hong Lew Chuen
Chief Executive Officer, Info-communications Media Development Authority of Singapore (IMDA)

Jon M. Huntsman
Vice-Chairman and President, Strategic Growth, Mastercard International

Dan Julian
Head of Privacy, ID.me

Hoda Al Khzaimi
Associate Vice-Provost for Research Translation and Entrepreneurship New York University Abu Dhabi

Ingrid Kopp
Co-Founder, Electric South

Eddie Liew
Senior Manager, Infocomm Media Development Authority (IMDA)

Mauro Miedico
Director, United Nations Counter-Terrorism Centre, United Nations Office on Counter Terrorism (UNOCT)

Sebastian Mosqueira
Director, Private Equity, The Olayan Group

Adriana Obregon
Government Affairs Senior Director, Incode Technologies

Judith Okonkwo
Founder, Imisi 3D

Apostolos Papadopolous
Chief Technology Officer and Senior Advisor to the Minister of Education, Government of Greece

Tim Roberts
Partner & Managing Director, UK Country Co-Leader, AlixPartners

Nilmini Rubin
Chief Policy Officer, Hedera Hashgraph

Luis Felipe Salin Monteiro
Global Vice-President, Government Affairs, Acesso Digital Tecnologia da Informação

Ian Slater
Executive Vice-President, Mastercard

Trisha Tan
Vice-President, Strategic Growth, Mastercard

Tan Kok Yam
Chief Executive Officer, SkillsFuture Singapore

Piotr Trabinski
Market Strategist, Macroeconomics, Google

Ethan Veneklasen
Head of Advocacy and Communications, ID2020

Priya Vora
Chief Executive Officer, DIAL

Larry Wade
Senior Director, Crypto/BC Risk & Compliance, PayPal

Royce Wee
Director, Department of Communications & Connectivity & Department of Data Protection, NEOM Company

Robby Yung
Chief Executive Officer, Animoca Brands

Endnotes

1. Runde, D. F., Murphy, E. L., & Bryja, T. (2024). Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition. *Center for Strategic and International Studies*. https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition
2. Srivathsan, B., Sorel, M., & Sachdeva, P. (2024). AI power: Expanding data center capacity to meet growing demand. *McKinsey & Company*. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand
3. ID.me. (n.d.). IRS and ID.me. https://help.id.me/hc/en-us/articles/8214940302999-IRS-and-ID-me
4. e-Estonia. (n.d.). ID-card. https://e-estonia.com/solutions/estonian-e-identity/id-card/
5. Hughes, A., Shandhi, M. H. H., Master, H., Dunn, J., & Brittain, E. (2023). Wearable devices in cardiovascular medicine. *Circulation Research*, 132(5), 652–670.
6. CLEAR. (n.d.). Which biometrics does CLEAR capture? https://www.clearme.com/support/which-biometrics-does-clear-capture
7. Be My Eyes. (n.d.). Be My Eyes for Smart Glasses. https://www.bemyeyes.com/be-my-eyes-smartglasses
8. Cloud Security Alliance. (2025, March 11). Agentic AI identity management approach. *Cloud Security Alliance*. https://cloudsecurityalliance.org/blog/2025/03/11/agentic-ai-identity-management-approach
9. Stadler, C. (2024). M-Pesa: Why the world's first large mobile payment platform keeps on winning. *Forbes*. https://www.forbes.com/sites/christianstadler/2024/06/11/m-pesa-why-the-worlds-first-large-mobile-payment-platform-keeps-on-winning
10. Raj, D. (2024). India's Unified Payments Interface has revolutionized its digital payments market. *Cornell University*. https://business.cornell.edu/hub/2024/12/20/indias-unified-payments-interface-has-revolutionized-its-digital-payments-market/
11. PYMNTS. (2025). Nearly half of consumers use digital wallets for bill payments globally. https://www.pymnts.com/digital-payments/2025/nearly-half-of-consumers-use-digital-wallets-for-bill-payments-globally
12. Capital One Shopping. (2025). Digital wallet statistics (2025): Users, growth rate & trends. https://capitaloneshopping.com/research/digital-wallet-statistics
13. Juniper Research. (2024). Digital Wallets Market 2024–2029. https://www.juniperresearch.com/research/fintech-payments/core-payments/digital-wallet-research-report
14. PR Newswire. (2024). International Telecommunication Union and Linux Foundation announce intent to launch the OpenWallet Forum. https://www.prnewswire.com/news-releases/international-telecommunication-union-and-linux-foundation-announce-intent-to-launch-the-openwallet-forum-302156383.html