INTERNET POLICY REVIEW

RESEARCH ARTICLE
OPEN ACCESS
PEER REVIEWED

Volume 15 **Issue** 3

Varieties of interoperability in the metaverse

Carolina Aguerre
Universidad Católica del Uruguay and CETYS, Universidad de San Andrés
caguerre@ucu.edu.uy
Joaquín Maquieira Alonzo *Fudan University* jmaqalonzo@gmail.com

DOI: https://doi.org/10.14763/2026.3.2120

Published: 24 September 2026
Received: 18 November 2025 **Accepted:** 31 July 2026

Funding: The authors did not receive any funding for this research.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Aguerre, C., & Maquieira Alonzo, J. (2026). Varieties of interoperability in the metaverse. *Internet Policy Review*, *15*(3). https://doi.org/10.14763/2026.3.2120

Keywords: Interoperability, Varieties, Platform governance, Geopolitics

Abstract: Interoperability has long been a central, though often overlooked, feature of digital systems. As visions of the metaverse evolve, it has become a key site of contestation. Some advocate for adversarial interoperability to break down platform lock-in and promote user freedom, while others warn that mandated openness could compromise security and reduce incentives for innovation. To make sense of these tensions, we propose a framework that links decisions about openness and closure to actor-specific economic and security goals. We identify 'Varieties of Interoperability' and illustrate this framework through structured examples from two components of the infrastructure layer – cloud and devices – drawn from publicly available corporate documents, policy reports, and scholarly analyses. Our analysis extends a prevalent narrative of corporate economic closure versus user-driven openness, showing that openness itself can also serve security-driven aims, such as coordination among trusted actors. The framework further suggests that, as geopolitical rivalries and digital sovereignty claims intensify, international security motivations may increasingly favor closure against rivals, raising the possibility of a fragmented 'splinterverse' rather than a unified global metaverse.

This paper is part of **Governing the metaverse through the lens of the public sphere**, a special issue of *Internet Policy Review* guest-edited by Annelieke A.M. Mooij and Sunimal Mendis.

I. Introduction

The metaverse has emerged as a prominent, yet contested vision of digital evolution, with no single definition prevailing among those shaping it. Ball (2022) presents it as a "massively scaled and interoperable network of real-time-rendered immersive virtual worlds that can be experienced synchronously and persistently" (p. 29) shared by unlimited users with continuity of data. The company co-founded by Neal Stephenson, who coined the term, describes it as the evolution of our lives online into richer 2D and 3D spaces to create, explore, socialise, and transact (Lamina1, 2023). From a scholarly perspective, Floridi (2022) approaches the metaverse primarily as an experiential environment, while identifying interoperability as one of its central challenges. Rather than constituting a universally agreed requirement, interoperability thus emerges as a point of contestation across different visions of the metaverse.

While interoperability is often defined as the ability of systems to share services or resources with other systems (Berg, 2024), there is a risk of embedding normativity as an inherently desirable outcome. If interoperability is instead approached as a site of contestation – where openness represents one side of a broader continuum – we may avoid a prescriptive lens on the issue, enabling a more nuanced reading of this phenomenon that captures the diverse forms and motivations underlying reduced interoperability. Several digital ecosystems today function as closed "walled gardens" that prioritise internal integration and limit external compatibility. Apple's Vision Pro, for instance, operates within a tightly controlled ecosystem, selectively constraining interoperability through its proprietary architecture. At the same time, interoperability can be enhanced in closed systems to connect trusted partners, as is the case of Apple's integration with Google's Gemini. These design decisions reflect the interests and values that shape technological development (Feenberg, 2008).

In this article we argue that interoperability, as a fundamental domain of contestation in contemporary digital governance, is decisive for the future of the metaverse. From this perspective, decisions about openness or closure reflect the economic and security priorities of different actors. States may support open systems to enhance innovation and growth while seeking closure to protect national infrastructure. Firms may embrace openness to expand markets or ecosystems, while imposing limits to protect intellectual property or reduce dependency. Users, too, face trade-offs: convenience and cost versus privacy and control.

Scholarship on open and closed systems is not new; management studies have long examined their organisational and strategic implications. Yet recent works increasingly address how such architectures shape power asymmetries among actors. Doctorow (2024) offers one critique of the decline of interoperability. He argues that the erosion of openness on the internet is not the result of technical limitations but of deliberate corporate and legal strategies that prevent users from connecting freely across systems.

While some emphasise the social and civic benefits of openness (Doctorow, 2024; Gasser & Palfrey, 2008), the geopolitical stakes of interoperability in a fluid artifact such as the metaverse have been sidelined. In an era of growing international security competition and digital sovereignty claims, decisions about openness and closure intersect more clearly with national goals (Pohle, 2025). States treat digital architectures as strategic assets: the control of digital infrastructures, standard-setting organisations, and platform ecosystems can shape global influence as much as trade or military power. With increasing weaponised interdependence (Farrell & Newman, 2019), interoperability is silently at the center of this competition.

In this scenario for competing markets and political control, conflicting visions of how the metaverse should be built and governed emerge (Egliston et al., 2024). Is the metaverse heading toward a pluralist integration of systems or toward fragmented, incompatible “metaverses”? How are economic and security priorities shaping these trajectories? To explore these questions, we analyse how various corporate actors support, shape, and interpret interoperability in this artifact. We ask, how do different actors and their priorities influence the development of architectures that either enable or constrain interoperability? Can we identify varieties of interoperability emerging at this stage?

To address these questions, this article is organised as follows. Section II draws on political economy approaches, digital platform studies, and geopolitics to show that struggles over openness and closure have long shaped digital governance, even if their implications have only recently become apparent. By bringing these perspectives together, we situate interoperability at the center of the paths for digital governance. Section III develops our framework and defines interoperability as a system-architecture choice shaped by actors’ economic and security interests. It then identifies the main dimensions and mechanisms through which these choices manifest. Section IV applies this framework to the infrastructure layer to show how different actors compete and cooperate in this regard. The final section concludes by discussing the implications of these findings for the future of digital governance.

II. Tracing interoperability: From platform ecosystems to weaponised digital infrastructures

While interoperability is often discussed as a desired goal, it is more accurately understood as a contingent outcome shaped by competing interests among users, firms, and governments. The struggles over openness and closure, as we will show, have always been present in business and digital platform literature. However, with the increasing geopolitical rivalry, it has become clearer that interoperability sits at the core of the international security competition and the weaponisation of interdependence. We draw on the literature on Varieties of Capitalism (VoC), platform ecosystems, and international relations to examine interoperability through different (metaverse) lenses and to recognise it for what it is: a central site of contestation in our digital world.

Interoperability within Varieties of Digital Capitalism

The VoC framework helps explain how institutional differences shape the coordination of digital infrastructures. Hall and Soskice (2001) argue that advanced capitalist economies differ in how firms coordinate their activities, distinguishing between *liberal market economies* and *coordinated market economies*. Each type relies on specific institutional complementarities that provide firms with distinct comparative institutional advantages in innovation and production. Thelen (2018) extends this logic to the platform economy, demonstrating that Uber's entry into the United States, Sweden, and Germany produced divergent outcomes because existing labour institutions and regulatory capacities structured the politics of platform work. From this perspective, Schmalz (2024) identifies distinct "varieties of digital capitalism" in the United States and China: a market-driven, corporate-led model versus a state-managed, security-oriented one. These institutional configurations, he argues, now underpin geopolitical competition as the United States deploys export controls and sanctions to limit China's technological expansion.

Recent work also shows how insights from the VoC tradition can be extended to strategic domains where economic and security considerations intersect. Drawing on VoC and state-business relations, Doppen et al. (2024) explain how different institutional configurations shape the balance between economic openness and the protection of assets under geopolitical competition. Our approach makes a more limited connection to this literature. We do not ask to what extent different varieties of capitalism explain different forms of interoperability – this remains a question for further research. Instead, we treat interoperability itself as a system-architecture choice shaped by actors' positions and perceptions of others, such as competitors and governments, and we illustrate how economic and security objectives (at firm and national level) can motivate both openness and closure. In practice, we show that great power rivalry increases "sovereignty" demands that result in selective interoperability with trusted partners.

Building on these studies, interoperability can be understood as one arena where these institutional logics are expressed. In Liberal Market Economies, firms tend to favour proprietary ecosystems and platform-led standards that align with market coordination and data monetisation. Coordinated Market Economies, exemplified by the European Union, pursue legally mandated openness – seen in measures such as the Digital Markets Act – to reconcile innovation with public oversight. China's state-managed digital capitalism, by contrast, encourages dense interoperability within domestic platforms while restricting external linkages to reinforce cyber sovereignty. As de Seta (2021) shows, this results not in a fully sealed "red stack" but in a layered topology of gateways, sieves, and domes that modulate participation in global networks under sovereign control. Across these cases, differences in institutional design generate distinct patterns of how – and for whom – interoperability is enabled or constrained.

We propose the notion of Varieties of Interoperability in the context of the metaverse, retaining the core VoC insight that institutional contexts shape coordination strategies among local actors but refocuses it on how mainly corporate and state actors position themselves in relation to interoperability. We approach interoperability not as a universally desired goal for firms or a feature inherently opposed by states, but as a system architecture choice positioned along an open–closed continuum. These choices reflect how states, firms, and individuals manage competition, innovation, privacy, and control through systems design. Our framework shifts the focus from the traditional VoC emphasis on labor markets and corporate finance to the tensions surrounding more open or closed system architectures. The result is a set of distinct forms of interoperability, shaped by ongoing tensions between the economic and security interests of different actors.

This perspective helps account for two central dynamics shaping the metaverse today: the profit-oriented structuration of digital environments through platform companies and the growing international securitisation of digital infrastructures (Lowry et al., 2025; Tu & de Castro e Silva, 2025; Doctorow, 2024). Across contexts, both firms and states weigh economic and security priorities when deciding whether to enable or constrain interoperability. Firms may close systems to protect strategic assets, limit exposure, or consolidate market power; states may promote openness to boost innovation or restrict flows to enhance resilience and local growth. Interoperability thus becomes a contested site where economic and security goals intersect – producing varied configurations of digital governance. We now turn to an approach from digital platform literature to show how these tensions are addressed from this viewpoint.

Platform power, boundaries, and infrastructural control

Platform power is central to understanding decisions around interoperability, particularly given the power asymmetries inherent in platform ecosystems. Due to their infrastructural centrality, platforms act as gatekeepers of services and how interoperability is understood. Platforms have emerged as dominant business models in response to capitalism's crisis of profitability, reorienting value creation around data and reorganising labour, production, and market access across sectors (Srnicek, 2017). The mechanisms of such platform power, including their gatekeeping functions and resistance to regulatory oversight, are particularly evident within the advertising ecosystem – central to the business models of two metaverse key players: Meta and Google. Here, platform firms exercise power by controlling data flows and dynamically tuning advertising delivery. Apple's App Tracking Transparency framework serves as a clear example, altering industry dynamics while paradoxically further entrenching Apple's own gatekeeping position (Nieborg & Poell, 2025).

In considering how firms strategically approach openness, Boudreau (2010) distinguishes two main paths: one involves "granting access" to outside innovators for developing complementary offerings around a controlled platform, while the other focuses on "devolving control" over key components of the platform itself. Expanding on this, Parker et al. (2016) refer to a spectrum of openness, emphasising that it is not a binary choice but a series of calibrations concerning user, developer, and sponsor participation. As Gawer (2021) argues, decisions over openness are inseparable from broader boundary choices involving the firm's scope, platform sides, and digital interfaces. These boundaries evolve interdependently as platforms mature – initially opening interfaces to stimulate complementarities and later recalibrating or closing them to consolidate control and profitability (Gawer, 2021).

Interoperability in digital ecosystems reflects how interdependence among actors is structured and governed. Research on ecosystem dynamics shows that the position of complements – whether upstream components or downstream applications – affects how firms coordinate and capture value, making the synchronisation of ecosystem evolution essential for interoperability to succeed (Adner & Kapoor, 2010). This coordination depends on more than shared standards: it involves decisions about who owns the platform, how much autonomy complementors have, and what mechanisms drive value creation (Hein et al., 2020). Interoperability, in this sense, is embedded in power-laden choices about openness and control. Apple's ecosystem strategy, for instance, shows that firms can retain tight control over core technologies while selectively opening up to third-party innovation – a balance that fosters interoperability on the firm's terms while excluding alternative configurations (Granstrand & Holgersson, 2020).

The boundaries between platforms, ecosystems, and infrastructures are increasingly blurred. This process termed *infrastructuralization* (Plantin et al., 2016) positions platforms as foundational to digital life. Plantin and De Seta (2019) extend this analysis to the Chinese context, showing how WeChat transitioned from a messaging app to a national infrastructure shaped by techno-nationalist policies and cyber-sovereignty agendas. The process of *super-appification* represents an intensified form of platform entrenchment and conglomeration across sectors and borders, consolidating services in a single interface (Van der Vlist et al., 2022). In this context, the race to control the emerging metaverse device stack – combining hardware, operating systems, and identity infrastructure – mirrors the logic of superapp consolidation but operates deeper in the architecture, offering platforms even greater leverage over how digital ecosystems evolve.

The infrastructural power of platforms is also exercised through interface governance, which is distinct from broader platform boundaries. While boundaries refer to the strategic scope of the platform, interfaces are the technical mechanisms that regulate how users and complementors interact with the platform (Gawer, 2021). Facebook, Application Programming Interfaces (APIs), have evolved from simple developer tools into complex, layered governance arrangements (Van der Vlist et al., 2022). These interfaces mediate what developers can do and therefore regulate the ecosystem itself – exemplifying both governance *of* and *by* platforms. This technicity is similarly evident in how platforms shape influencer economies: platforms use interface features to manage how commercial content is labelled and who is responsible for following the law. This reveals tensions between governance *of* platforms (legal frameworks) and governance *by* platforms (technical and interface-based control) (Annabell et al., 2024). Beyond individual platforms, protocol power (Crawford, 2024) addresses how dominant actors use technical standards to define inclusion and manage interoperability on their terms. While such protocols appear to promote openness, they often enable new forms of data extraction, lock-in, and subscription-based monetisation (Crawford, 2024).

The literature presented so far, although highly valuable for our study, either overlooks the competing interests surrounding interoperability or fails to account for the power asymmetries among different actors. Filling this gap, Doctorow (2024) argues that general-purpose computers are inherently capable of running interoperating software, making purely technical barriers to interoperability ultimately insufficient. Instead, dominant firms rely on legal restrictions and corporate strategies to prevent unauthorised interconnection. He stresses how dominant firms use intellectual property laws, especially anti-circumvention provisions like Section 1201 of the Digital Millennium Copyright Act, to block third-party interconnection and user control. This “legal impossibility,” rather than a technical one, makes interoperability a political and economic battleground. Consequently, a call for legal protections for adversarial interoperability or competitive compatibility comes from Doctorow (2024), who defines it as creating compatibility with existing systems without permission – typically via reverse engineering – as a path to restore user agency and enable real competition.

The discussion so far has focused on how platform firms and users deal with the open/closed dilemma of interoperability, with motivations broadly based on economic and efficiency incentives on one hand and control and security on the other, but for a commercial purpose. While this perspective highlights important aspects of digital ecosystems, the strategic thinking of firms and the aims of users are increasingly influenced by international security competition among major powers. Consequently, the criteria for assessing interoperability have shifted, intensifying national security needs. In this scenario, platforms can become both places for and tools of influence, changing how states consider the benefits of openness against the perceived security advantages of more controlled ecosystems or those based on strong national companies. The following section examines this international aspect, focusing on how states’ different security and economic goals change the socio-technical context for interoperability and the role digital platforms play in achieving state objectives.

Interdependence, security competition, and digital sovereignty

The liberal vision of institutionalised openness that once supported global economic and technological integration since the end of WWII now faces a growing legitimacy crises and political backlash (Börzel & Zürn, 2021; Ikenberry, 2018). These pressures directly affect how states and firms understand and enact interoperability. Openness through shared technical standards and cooperative regimes, once a normative extension of liberal order, is now a contested terrain shaped by competing governance logics. In the metaverse, decisions about whether and how to interoperate are increasingly entangled with broader geopolitical transformations where security concerns are baked into the policy choices of networked digital technologies. This understanding of interoperability as a contested political terrain is echoed by Bellanova et al. (2026), who conceptualise it as a technopolitical process through which power is redistributed and contested. Their focus on database interoperability as a statecraft issue, however, leaves broader variation across actors and ecosystems less explored.

In response to the perceived erosion of state authority in the digital realm and the vulnerabilities exposed by foreign surveillance, the concept of "digital sovereignty" has gained prominence (Couture & Toupin, 2019; Pohle & Thiel, 2020; Pohle, 2025). A key strategy in asserting digital sovereignty is data localisation, where states mandate that citizens' data be stored and processed within national borders, aiming to enhance regulatory oversight and national security (Wu, 2021). These efforts are often tangled with economic strategies described by Mueller and Farhat (2022) as "digital neo-mercantilism," where states use protectionist measures and promote national champions to build domestic digital industries and reduce reliance on foreign technology providers.

The geopolitical implications of digital platforms are made clear by the global expansion of major Chinese technology firms and the resulting international controversies (Cartwright, 2020). Efforts to govern Chinese technologies are increasingly framed by a broader range of concerns, including national and data security alongside foreign interference, and the assertion of technological sovereignty based on varied legal and policy narrations (Bernot et al., 2024). At the same time, the TikTok controversy highlights how policy responses often emphasis e geopolitical motivations, potentially obscuring other factors like the value of competition in highly concentrated digital markets (Gray, 2021). This platform-centric geopolitical competition is further exemplified by China's distinct vision for "cyber sovereignty" (Segal, 2020; Creemers, 2020). However, this assertion of sovereignty does not occur in a vacuum, as China's approach to internet governance is also shaped by reactions to and interactions with existing global rules, which are often US-made (Tusikov, 2019). These varying approaches contribute to divergent platform ecosystems with unique historical and developmental logics, challenging Western-centric models of platform studies (Davis & Xiao, 2021; Gray & Tang, 2025).

This rise of distinct, geopolitically shaped platform ecosystems and competing approaches to digital governance poses serious challenges to metaverse interoperability. If major powers promote metaverse development aligned with their specific cyber sovereignty doctrines or seek to advantage national platform champions, the result could be the emergence of incompatible metaverse “blocs” or “splinternets.”

The weaponisation of digital interoperability starts with states increasingly asserting control over digital infrastructures – often privately operated systems that were once treated as neutral (Ortiz-Freuler, 2023, 2025; Mann & Daly, 2020). But these infrastructures are not simply shaped by power. They also have agentic capacity to enable, block, or redirect political goals. This capacity comes from the way past decisions are embedded in their technical and institutional design (De Goede & Westermeier, 2022). As a result, when states try to use these systems for strategic purposes, they often encounter resistance from the private firms that own or operate them. These firms may push back when government demands threaten their business interests (Gjesvik, 2022).

One way in which states exert influence is by targeting key control points in digital networks – such as payment systems or online platforms – to block or limit access (Tusikov, 2021). This approach has expanded into areas like advanced semiconductors and 5G, where countries use their positions in global supply chains to restrict competitors (Calcara, 2023; Segal, 2021). For example, controlling the chip design stage gives certain states leverage over other parts of the supply chain, including the assembly and distribution of final products (Beaumier & Cartwright, 2024). These tactics, however, can trigger strong reactions. Targeted countries often respond by investing in their own technologies and reducing their dependence on foreign systems, which may push the world closer to a split into separate digital and technological zones (Woods, 2025). As Beaumier and Gjesvik (2025) argue, governments trying to manage this situation face a difficult balancing act between keeping regulatory control, supporting competitive markets, and maintaining open digital systems under increasing geopolitical pressure.

III. Varieties of interoperability for the metaverse

The previous section shows that debates over interoperability have long been present in the fields of business administration, information systems, and communications, and international relations. To make better sense of the tensions around it, this section introduces our framework, which defines interoperability as a system architecture choice shaped by actors' goals, positions, and perceptions. We use this lens to identify emerging varieties of interoperability and to show how they reflect different trade-offs between openness and control in the metaverse based on institutional logics, platform choices, and geopolitical interpretations.

We adopt a qualitative, theory-building approach to develop the "Varieties of Interoperability" framework, linking system design choices to state and corporate actors' economic and security motivations (Hoon, 2013; Markus et al, 2002). The framework is applied through structured illustrations drawn from publicly available corporate documents, policy and press reports, and scholarly analyses of digital infrastructures, platforms, and metaverse technologies. The empirical material in this article functions as illustrative examples rather than case studies in the methodological sense (Yin, 2009). Following conventions in explanatory typologies (Elman, 2005), each example is selected because it instantiates one cell of the Varieties of Interoperability typology (Table 1), allowing us to demonstrate the framework's analytical potential, rather than to establish causal or comparative claims about firm behaviour. The examples are illustrative and heuristic to show that the typology can be populated from the wider group of metaverse-relevant firms. Inclusion criteria for the firms analysed in section IV were: the fit with the typology, to avoid extensive interpretative stretching; relevance to the layer under examination, i.e. restricted to the two layers to be analysed in sections III and IV though in some cases these firms are notorious players in other layers, notably data; and finally, public documentation availability and market salience, to provide more consequential interpretation and legibility for readers.

Interoperability as a context-driven choice of preferences

Our framework approaches interoperability as a system architecture decision made by firms, governments, and users within socio-technical contexts. We identify three interrelated factors that shape these decisions:

1. Goals: Actors may pursue economic objectives such as innovation, growth, and efficiency or security interests such as data protection, infrastructure resilience, or safeguarding privacy.[1]
2. System Position: Actors occupy different roles within the digital architecture – such as dominant platforms, hegemonic states, complementary providers, rising challengers, or end-users. Their position

1. Security-oriented goals are used here as an umbrella category encompassing different forms and levels of protection – from individual privacy and data protection to national security – rather than as a single type of security (Kshetri, 2026).

shapes how they perceive the risks and opportunities of interoperability.
3. Perception of Others: Trust, alignment, rivalry, or uncertainty with other actors influences whether connections are built or avoided.

These three elements interact to produce interoperability preferences. As illustrated in Table 1, both openness and closure can serve either economic or security-oriented designs. For instance, opening a system to new entrants can stimulate competition and innovation, but opening only to trusted actors may strengthen collective resilience against threats. Conversely, closure can protect a firm's competitive advantage, or it can defend national infrastructure from foreign influence.

TABLE 1: Design rationales for openness and closure across actor priorities

	ECONOMIC-ORIENTED DESIGN	SECURITY-ORIENTED DESIGN
OPENNESS	Open to new entrants to grow the ecosystem, lower user switching costs, or enable wider access to services and markets.	Open to trusted actors to coordinate responses to threats, share technical standards, or build mutual resilience.
CLOSURE	Close access to preserve competitive advantage, prevent imitation, or keep users and data within one ecosystem.	Close to rivals or unverified actors to avoid manipulation, content threats, or dependence on foreign infrastructure.

Because openness and closure can serve different goals at once, the reasons behind these choices are often mixed. A move toward openness might aim to expand the ecosystem with new players or to build resilience through cooperation with trusted actors. Likewise, closing access might reflect concern about unreliable partners or a strategy to protect competitive advantage. Each choice tends to reflect a mix of pressures, with trade-offs between growth, control, trust, and risk shaping the final decision.

Finally, these choices are not always perceived in the same way by every actor. For example, a company may say it limits access to protect users or ensure safety, while others may see it to block competition. This motivational framing shows that interoperability decisions are open to different interpretations (Egliston et al., 2024). This framework's contribution is twofold: treating openness/closure as cross-cutting to economic/security motive rather than assuming that openness equates to economic/liberal and closure to security/protectionist; and secondly, showing security motives can drive openness (trusted-partner coordination), which the existing literatures do not anticipate or stay focused on the national–strategic level.

Dimensions of interoperability

From the literature review, we identified six critical dimensions of interoperability relevant to digital systems and the metaverse: vertical/horizontal, symmetrical/asymmetrical, general/ecosystem, syntactic/semantic, technical/political, and the various modes of achieving interoperability. These are developed in Table 2.

TABLE 2: Dimensions of interoperability

DIMENSION PAIR	CORE DISTINCTION	EXAMPLE
VERTICAL / HORIZONTAL	Across layers of the stack vs. between services at the same layer	Vertical: multiple app stores on one OS; Horizontal: cross-platform messaging (Bourreau, Krämer, & Buiten, 2022)
SYMMETRICAL / ASYMMETRICAL	Equal vs. unequal capacity to interoperate	Facebook's one-way cross-posting (Bourreau, Krämer, & Buiten, 2022)
GENERAL / ECOSYSTEM	Seamless interoperation between distinct systems vs. deep integration read externally as one environment	GI: shared protocols (Berg, 2024); Ecosystem: military/high-stakes domains (Ferreyra, 2025; Pernin et al., 2020)
SYNTACTIC / SEMANTIC	Shared structure enabling legibility vs. shared meaning enabling interpretation	Common ontologies for "price," "identity," "location" (Gasser, 2015; Berg, 2024)
TECHNICAL / POLITICAL	Material capacity to interconnect vs. regulatory enabling/blocking of that capacity	EU Digital Markets Act mandate (DeNardis, 2011)

Modes of achieving interoperability

How interoperability is achieved also matters. We distinguish four primary modes: cooperative, mandated, adversarial, and indifferent.

TABLE 3: Modes of achieving interoperability

MODE	TRIGGER	CAN PRODUCE	EXAMPLE
COOPERATIVE	Voluntary agreement, shared incentives	Openness	Industry alliances, shared APIs (Doctorow, 2024)
MANDATED	State regulatory authority	Openness *or* closure	DMA (openness); export controls, classified-network standards (closure) (Ott et al., 2026; Wu, 2021; Beaumier & Cartwright, 2024)
ADVERSARIAL	Unauthorised reverse engineering, legal gray areas	Openness (imposed on an unwilling incumbent)	Browser and device compatibility history (Doctorow, 2024)
INDIFFERENT	No active design choice either way	Either, by default	Backward-compatible hardware/software (Doctorow, 2024; Gasser, 2015)

Understanding interoperability in the metaverse requires recognising its many dimensions and ways of achieving it by different actors. These system design decisions are shaped by the actors' goals, positions, and perceptions.

These four modes account for interoperability outcomes driven by the focal actor's own agreement, a state's regulatory authority, unilateral circumvention, or simple non-design. They do not accommodate cases in which a third actor's market power forces an otherwise unwilling firm to open access. We return to this possibility, and the device-layer case that motivates it, in the conclusion.

IV. A layered approach to actors' decisions in the metaverse

In this section we apply our framework to the infrastructure layer to show how competing actors' priorities shape openness and closure. We focus on cloud and devices because they represent the backend and user-facing ends of the layer, while further research could extend the analysis to connectivity infrastructure, such as fiber-optic cables, satellites, Wi-Fi networks, and mobile base stations. These two layers are where economic and security tensions are currently most publicly documented, most foundational for everything built above them and where both firm and state actors already intervene, leaving protocol and content layers, addressed only briefly here, to future work.

Cloud

The cloud layer structures how data is stored, processed, and accessed across metaverse platforms. Economically, openness can help firms scale and reach more users, while closure can keep more value within the firm. *Table 4* provides an example of infrastructure openness serving economic goals. While part of their services run in a private Roblox Cloud, the company also uses public cloud – mostly AWS – for global services and additional capacity, including GPUs for AI (Roblox, 2026). By contrast, Xbox Cloud Gaming relies on Azure and custom Xbox server hardware, allowing Microsoft to build the service on top of its existing global cloud infrastructure rather than depend on external providers (Choudhry, 2019).

Closure can serve security goals through selective interoperability. As *Table 4* illustrates, Apple's partnership with Google allows to incorporate Gemini models and cloud infrastructure while keeping inferences within Apple devices – including Apple Vision Pro – or their Private Cloud Compute, in line with Apple's privacy focus (Leswing, 2026). In a more closed, security-driven architecture, Palantir and NVIDIA offer a "Sovereign AI" architecture to keep AI capabilities within customer-managed environments, supporting digital twin platforms with local control (Palantir, 2026).

The use of open-weight AI models under Sovereign AI illustrates how openness can support a closed design architecture. Open-weight models can be deployed locally to reduce reliance on external providers. This is particularly relevant to metaverse interoperability, where such models can operate within closed environments managing sensitive data and digital twin applications. Openness at the model level thus supports security-oriented closure at the infrastructure level, reducing dependence on unreliable actors while retaining advanced capabilities.

TABLE 4: Interoperability choices in metaverse cloud infrastructure (Sources: Palantir, 2026; Roblox, 2026; Choudhry, 2019; Leswing, 2026; Reuters, 2025)

	ECONOMY-ORIENTED	SECURITY-ORIENTED
OPENNESS	Roblox combines its private Roblox Cloud with AWS public-cloud capacity, including expanding GPU infrastructure in the public cloud for AI, to improve scalability and efficiency.	Apple connects users to Google's Gemini through a privacy-preserving system. The setup allows openness but only to a trusted partner.
CLOSURE	For Xbox Cloud Gaming, Microsoft integrates proprietary Xbox servers with Azure's global reach, reducing reliance on external providers while retaining value capture.	Palantir and NVIDIA offer 'Sovereign AI' infrastructure for operational and digital-twin environments, keeping sensitive data and models within customer-controlled systems.

This variety of strategies offers useful context, but additional insights emerge when we examine a single actor's decisions. *Table 5* illustrates this dynamic through Meta's architectural design for Quest's use of cloud infrastructure, showing how a single decision can reflect multiple, sometimes competing, priorities. Meta embraces the openness of public cloud infrastructure to achieve economic goals, leveraging AWS's global reach to scale the service quickly and affordably (Moss, 2021). Simultaneously, it relies on AWS's established security frameworks to meet enterprise standards (Bharathan, 2025). On the other hand, this openness is carefully balanced with a more closed design. To protect its economic ecosystem, Meta restricts interoperability through proprietary avatar systems and APIs. From a security perspective, the most sensitive biometric data – such as hand or body movement (Meta, 2025a) and raw eye-tracking (Meta, 2025b) – is allowed to be processed exclusively on-device to minimise privacy risks. These layered decisions illustrate how Meta navigates the continuum between openness and closure, using interoperability as both a tool for market expansion and a mechanism for security assurance within its metaverse infrastructure.

TABLE 5: Interoperability trade-offs in Meta's use of cloud infrastructure (Sources: Meta, 2025a, 2025b; Lee, 2025)

	ECONOMY-ORIENTED	SECURITY-ORIENTED
OPENNESS	Meta uses AWS's global cloud infrastructure to scale Horizon Workrooms quickly and affordably, optimising for reach and performance.	Relies on AWS compliance frameworks (e.g., SOC 2, FedRAMP) to meet enterprise security standards and ensure trust in cloud-based collaboration.
CLOSURE	Restricts interoperability by using proprietary avatar systems, APIs, and data formats to protect platform value and revenue.	Allows processing and storing certain biometric data (e.g., raw eye-tracking, hand movements) exclusively on Quest devices, avoiding cloud upload to minimise privacy risks.

Devices

In Table 6, different architecture design decisions are made explicit by weighing economic and security goals. On the economy-oriented side, Qualcomm's Snapdragon XR chips illustrate how openness can support market growth. These chips power Meta's Quest 3 headset and other extended-reality devices such as those from HTC and Pico, enabling manufacturers to build XR products across various markets (Hollister, 2023). This strategy helps expand the ecosystem and attract users, even if it means enabling foreign rivals to grow. By contrast, Sony's PlayStation ecosystem long restricted cross-platform features such as cross-play and cross-purchasing to protect its dominant market position and sustain user lock-in. The company resisted interoperability for more than a decade, fearing that if players could interact with users on rival platforms, they might have less incentive to buy a PlayStation, until market pressure from *Fortnite* eventually forced it to relax these policies (Ball, 2022).

Security concerns push in a different direction, often favoring more control. The military AR headset is a clear example of security-oriented closure: it runs on a locked operating system within a private military network to protect sensitive information and avoid hacking. However, not all security-focused strategies rely on full closure. Stryker, a medical technology company, builds its surgical planning software on the Apple Vision Pro. This is a form of selective openness – it allows interoperability, but only with a trusted partner known for privacy and reliability (Apple, 2024). Taken together, these cases show how decisions at the device layer map onto a continuum between openness and closure, reflecting how actors weigh economic incentives for market expansion against security imperatives of control and protection.

TABLE 6: Interoperability trade-offs in metaverse devices (Sources: Google Cloud, 2025; Apple, 2024; Choudhry, 2019, Segal, 2020, Lee, 2025)

	ECONOMY-ORIENTED	SECURITY-ORIENTED
OPENNESS	Qualcomm's Snapdragon XR2 chip powers Meta's Quest 3 headset as well as XR	Stryker's Use of Apple Vision Pro: The medical tech company Stryker builds

	ECONOMY-ORIENTED	SECURITY-ORIENTED
	devices from HTC and the Chinese company Pico (ByteDance). By supplying core components to both Western and Chinese manufacturers, Qualcomm favors a market-expanding strategy that prioritises revenue growth over geopolitical fragmentation.	its surgical planning software on the Vision Pro. This represents an openness to leveraging a trusted partner's secure, high-performance platform to ensure patient data privacy and reliability, rather than developing proprietary hardware.
CLOSURE	Video game consoles (PlayStation): The hardware is sold at low margins to build a loyal user base. Profit relies on a closed ecosystem of exclusive games and digital stores that limit cross-platform features, ensuring users remain within the platform's network.	Military AR headset: A ruggedised headset for soldiers that overlays classified maps and drone feeds. The device runs a locked-down OS on a closed military network to prevent hacking or data leaks. The goal is mission security through extreme hardware and software closure.

State-level standard-setting shows the same mandate mechanism serving opposite goals. China's Ministry of Industry and Information Technology has convened a Metaverse Standardisation Technical Committee to align domestic XR standards with the state's digital-sovereignty and industrial-policy goals (Gray & Tang, 2025). The EU's Digital Markets Act mandates interoperability toward the opposite end: strengthening competition among rival firms rather than coordinating a national industrial base (Ott et al., 2026). The same mode can therefore serve either security/sovereignty or economic-competition goals, depending on which actor sits behind it.

Qualcomm's licensing of its Snapdragon XR2 chip to Meta, HTC, and Pico (ByteDance) illustrates vertical, cooperative interoperability that persists even where it strengthens a geopolitical rival. The chip is supplied under standard commercial terms to all three manufacturers (Hollister, 2023): the relationship sits vertically between the component and device layers, is general rather than ecosystem-bound, and is symmetric in its terms of access even as it remains asymmetric in power, since Qualcomm sets the specifications and royalty terms that downstream manufacturers must design around. This cuts against the expectation, implicit in weaponised-interdependence accounts (Farrell & Newman, 2019) and in Schmalz's (2024) account of a US-China split into competing technological spheres, that dominant infrastructure providers converge on closure toward rival-aligned firms as security competition intensifies. Qualcomm's continued cooperative openness toward a ByteDance-linked manufacturer shows that firm-level economic logic can persist independently of, and even in tension with, state-level security logic, surfacing the cross-cutting dynamic of the Varieties of Interoperability framework, rather than an outcome either the VoC or weaponised-interdependence literatures would predict alone. However, that openness is not unconditional as it holds only within the current US export-control regime for semiconductors and could shift from cooperative to mandated closure if controls were extended from advanced logic chips (Beaumier & Cartwright, 2024) to XR-specific silicon, which is a reminder that even firm-level economic openness operates inside a security perimeter set by states.

Meta’s cloud infrastructure decisions show that a single firm can hold contradictory interoperability postures simultaneously across layers: cooperative openness at the infrastructure layer, ecosystem-level closure at the application layer, and technical closure for privacy reasons at the data layer. At the infrastructure layer, Meta’s reliance on AWS is vertical interoperability, general rather than ecosystem-bound, and cooperative in mode, adopted for both economic reach (Moss, 2021) and to inherit AWS’s compliance frameworks such as SOC 2 and FedRAMP (Bharathan, 2025). At the application layer, Meta’s proprietary avatar systems and APIs produce horizontal closure relative to rival platforms through ecosystem interoperability logic that keeps users, developers, and data inside Meta's own environment (walled garden). At the data layer, a third logic operates processing sensitive biometric data such as hand, body, and eye tracking exclusively on-device (Meta, 2025a, 2025b) where technical interoperability is deliberately constrained for political and privacy reasons. Existing accounts of platform boundaries generally treat openness and closure as a single, coherent stance a firm periodically revises (Gawer, 2021; Boudreau, 2010). Yet the case of Meta shows this is too broad, since the same firm is simultaneously cooperative-open, ecosystem-closed, and ‘technically closed for privacy’ across three layers at once, each governed by a distinct logic.

Sony’s decade-long resistance to cross-play, and its eventual reversal, shows that closure can persist as a stable economic strategy and then convert to openness through coercion by a third party’s market power. PlayStation’s restriction of cross-play and cross-purchase is horizontal closure competing consoles at the same layer sustained through ecosystem interoperability logic that binds hardware, games, and network services into a single loyalty structure, pursued for purely economic reasons with no security rationale involved (Ball, 2022), is a relevant contrast to Qualcomm’s economic openness and Meta’s mixed economic/security case. For over a decade Sony simply did not build cross-play capability, which served the same competitive purpose as actively blocking it. Parker et al.’s (2016) account of a firm calibrating its “spectrum of openness” assumes the firm itself controls the pace and direction of that calibration; Sony's reversal breaks this assumption, since cross-play was not opened through voluntary recalibration or regulatory mandate, but because Fortnite's cross-platform popularity made refusing it a competitive liability severe enough to force Sony's hand. This is neither cooperative nor mandated, where a third-party platform's leverage over end users functions like a de facto mandate without any state involved, that we label as "market-coerced" interoperability.

The military headset and Stryker's use of the Vision Pro show that security motives do not converge on a single design response, as identical goals, i.e. protecting sensitive data, produce opposite architectures depending on how the actor perceives the other party. The military headset is a case of total ecosystem closure under a de facto mandate: a state security requirement locks the operating system to a private network and forecloses external interoperability entirely, exemplifying the "high-stakes collaborative domains" (Ferreyra, 2025; Pernin et al., 2020). Stryker's case is structurally different: it is vertical interoperability across sectors, asymmetric in power, and cooperative in mode, resting on a political and technical compliance layer where Apple's privacy and security posture meets the regulatory rules Stryker's software requires (Apple, 2024). While both actors are security-motivated there is a difference in system position and perception of others: the military actor treats every outside party as an undifferentiated threat, producing zero-trust closure, while Stryker treats Apple specifically as a trusted partner, producing openness bounded to that single relationship. Yet, while from Stryker's position this is security-oriented openness, for Apple the same relationship is economy-oriented closure, since its walled garden is what makes it a credible "trusted partner" in the first-place system position, dominant platform versus downstream complementor. However, the headset's closure is not closure to everyone, since receiving classified maps and drone feeds requires some standardised data link to allied command-and-control systems, and Stryker's openness is not fully its own to extend or revoke; because the relationship is asymmetric, the selective openness it enjoys is a grant from Apple that could be narrowed unilaterally.

The Varieties of Interoperability framework provides a lens to reinterpret what drives openness and closure across and within layers. It moves beyond viewing interoperability as an inherently desirable goal, showing instead how design decisions reflect distinct economic and security incentives. On the one hand, as it has already been well documented in the literature, the erosion of openness on the internet stems largely from deliberate corporate and legal strategies aimed at revenue growth and value capture. These economic forms of closure, visible in proprietary standards and platform lock-ins, limit user autonomy and cross-system connectivity. Yet, our framework helps highlight increasing closure under international security motivations instead of market and revenue growth. With growing weaponisation, actors increasingly restrict interoperability for security reasons, insulating infrastructures, data flows, and supply chains to reduce geopolitical vulnerability. Interoperability is increasingly restricted for security rather than economic reasons.

On the other hand, the framework helps visualise why, even with rising geopolitical competition and weaponised interdependence, many actors continue to pursue selective forms of openness. It highlights that openness can itself be pursued under security-oriented goals, as states and firms increasingly rely on trusted partners to ensure resilience, coordination, and control. They do so through different dimensions and modes of interoperability across layers. At the infrastructure and protocol levels, some maintain open standards and shared technical foundations to guarantee redundancy and baseline connectivity while enforcing political constraints over data flows, or network participation, or governance access. Others rely on cooperative or mandated openness, using regulations, trade partnerships, or military alliances to preserve interoperability within controlled networks. These cases show that open interoperability can serve both security and economic objectives, functioning as a mechanism of coordination as much as of control. Rather than prescribing openness or closure, the framework exposes the coexistence of multiple varieties of interoperability, each reflecting different combinations of economic incentives and security concerns that unfold in companies and states from both the United States and China.

V. Conclusion

In this article we examined interoperability as a domain where economic and security motivations intersect, shaping the architecture and governance of digital systems. By linking openness and closure to actors' strategic goals, positions, and perceptions, we have shown how decisions about interoperability express broader priorities – innovation, control, trust, and resilience – rather than mere technical compatibility. These decisions define how states, firms, and users negotiate interdependence in a digital environment increasingly structured by international security concerns.

Applied to the metaverse, this framework reveals multiple varieties of interoperability rather than a single model of interconnectivity. Across the infrastructure layer, actors pursue different combinations of openness and closure that reflect their interests and power positions. With the growing weaponisation of interdependence, many actors restrict interoperability for security reasons, insulating infrastructures, data flows, and supply chains to reduce geopolitical vulnerability. At the same time, openness is increasingly pursued under security-oriented goals, as states and firms rely on trusted partners to ensure stability within controlled networks. Future work can expand this framework to the protocol and content layer of the metaverse.

We have shown that interoperability stands silently at the center of digital governance and metaverse imaginaries (Hou, 2025). The argument advanced here suggests that, while in the past openness features of interoperability in digital platforms and digital networks were an inherently desirable goal, in the current context in which the metaverse is unfolding, it is more productive to trace how different actors pursue their own varieties of interoperability amid shifting economic and security motivations.

Though this work has not been able to address all the layers of the metaverse, nor the different actors, the analysis surfaces a limit in the framework's own typology of modes. Sony's decade-long resistance to PlayStation cross-play, and its reversal under pressure from Fortnite's cross-platform popularity, does not fit cleanly into any of the four modes developed in Section III, suggesting a fifth mode, that could be labelled as market-coerced interoperability, in which a third-party platform's leverage over the shared user base functions as a de facto mandate, forcing a firm to open access despite no change in its economic calculus and no state involvement. The four modes identified here should be read as an initial, not exhaustive approach to the typology. Further work is needed to establish how common market-coerced interoperability is unfolding, incorporating literature from competition and anti-trust.

Despite this and other limitations, this article provides a preliminary foundation from which to continue exploring the different choices and scenarios on metaverse and digital infrastructures interoperability discussions, that are at the core of digital governance debates. Future debates in different scholarly and policy venues should focus less on restoring the ideal of openness and more on managing the emerging varieties of interoperability that this article has surfaced, which will define the next phase of this still inchoate technical artifact and the networked ecosystem.

ACKNOWLEDGEMENTS

Disclosure of AI use: The tables in Section III (tables 2 and 3) were drafted with the assistance of Claude Sonnet 5 and subsequently revised and verified by the authors.

References

Adner, R., & Kapoor, R. (2010). Value creation in innovation ecosystems: How the structure of technological interdependence affects firm performance in new technology generations. *Strategic Management Journal*, *31*(3), 306–333. https://doi.org/10.1002/smj.821

Annabell, T., Aade, L., & Goanta, C. (2024). (Un)disclosed brand partnerships: How platform policies and interfaces shape commercial content for influencers. *Internet Policy Review*, *13*(4). https://doi.org/10.14763/2024.4.1814

Apple Newsroom. (2024, March 11). *Apple Vision Pro unlocks new opportunities for health app developers*. Apple Newsroom. https://www.apple.com/newsroom/2024/03/apple-vision-pro-unlocks-new-opportunities-for-health-app-developers

Badasyan, N., & Chakrabarti, S. (2008). A simple game-theoretic analysis of peering and transit contracting among internet service providers. *Telecommunications Policy*, *32*(1), 4–18. https://doi.org/10.1016/j.telpol.2007.11.002

Ball, M. (2022). *The metaverse: And how it will revolutionize everything*. Liveright Publishing Corporation.

Beaumier, G., & Cartwright, M. (2024). Cross-network weaponization in the semiconductor supply chain. *International Studies Quarterly*, *68*(1). https://doi.org/10.1093/isq/sqae003

Beaumier, G., & Gjesvik, L. (2025). Digital governance in a rubber band: Structural constraints in governing a global digital economy. *Global Studies Quarterly*, *5*(2). https://doi.org/10.1093/isagsq/ksaf043

Bellanova, R., Passoth, J.-H., & Pollozek, S. (2026). The technopolitics of database interoperability. *Big Data & Society*, *13*(2), 1–6. https://doi.org/10.1177/20539517261451457

Berg, C. (2024). Interoperability. *Internet Policy Review*, *13*(2). https://doi.org/10.14763/2024.2.1749

Bernot, A., Cooney-O’Donoghue, D., & Mann, M. (2024). Governing Chinese technologies: TikTok, foreign interference, and technological sovereignty. *Internet Policy Review*, *13*(1). https://doi.org/10.14763/2024.1.1741

Bharathan, R. (2025). *Security controls compliance cloud security, AI, and LLMs – AWS, Azure, Google Cloud GCP*. Technical Disclosure Commons. https://www.tdcommons.org/dpubs_series/7758

Börzel, T. A., & Zürn, M. (2021). Contestations of the liberal international order: From liberal multilateralism to postnational liberalism. *International Organization*, *75*(2), 282–305. https://doi.org/10.1017/S0020818320000570

Boudreau, K. (2010). Open platform strategies and innovation: Granting access vs. Devolving control. *Management Science*, *56*(10), 1849–1872. https://doi.org/10.1287/mnsc.1100.1215

Bourreau, M., Krämer, J., & Buiten, M. (2022). *Interoperability in digital markets*. Centre on Regulation in Europe. https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf

Calcara, A. (2023). From quiet to noisy politics: Varieties of European reactions to 5G and Huawei. *Governance*, *36*(2), 439–457. https://doi.org/10.1111/gove.12674

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1494

Choudhry, K. (2019, May 24). *Project xCloud: More for gamers and developers*. Microsoft Xbox Wire. https://news.xbox.com/en-us/2019/05/24/project-xcloud-more-for-gamers-and-developers/

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Crawford, C. (2024). Protocol power: Matter, IoT interoperability, and a critique of industry self-regulation. *Internet Policy Review*, *13*(2). https://doi.org/10.14763/2024.2.1776

Creemers, R. J. E. H. (2020). China's conception of cyber sovereignty: Rhetoric and realization. In D. Broeders & B. Van Den Berg (Eds), *Governing cyberspace: Behavior, power, and diplomacy* (pp. 107–142). Rowman & Littlefield.

Davis, M., & Xiao, J. (2021). De-westernizing platform studies: History and logics of Chinese and US platforms. *International Journal of Communication*, *15*, 103–122.

De Goede, M., & Westermeier, C. (2022). Infrastructural geopolitics. *International Studies Quarterly*, *66*(3). https://doi.org/10.1093/isq/sqac033

De Seta, G. (2021). Gateways, sieves, and domes: On the infrastructural topology of the Chinese stack. *International Journal of Communication*, *15*, 2669–2692.

DeNardis, L. (Ed.). (2011). *Opening standards: The global politics of interoperability*. MIT Press.

Doctorow, C. (2024). *The internet con: How to seize the means of computation*. Verso Books.

Doppen, F., Calcara, A., & De Bièvre, D. (2024). Balancing security and economics: Domestic state-firm relations and investment screening mechanisms in Europe. *Review of International Political Economy*, *31*(6), 1637–1661. https://doi.org/10.1080/09692290.2024.2368601

Egliston, B., Carter, M., & Clark, K. E. (2024). Who will govern the metaverse? Examining governance initiatives for extended reality (XR) technologies. *New Media & Society*, *27*(6), 3361–3381. https://doi.org/10.1177/14614448231226172

Elman, C. (2005). Explanatory typologies in qualitative studies of international politics. *International Organization*, *59*(2), 293–326. https://doi.org/10.1017/S0020818305050101

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Feenberg, A. (2008). From critical theory of technology to the rational critique of rationality. *Social Epistemology*, *22*(1), 5–28. https://doi.org/10.1080/02691720701773247

Ferreyra, M. (2025). A knowledge taxonomy for military interoperability: The United States and

Brazil in peacekeeping and stabilization operations. *Armed Forces & Society*, *0*(0). https://doi.org/10.1177/0095327X251347176

Floridi, L. (2022). Metaverse: A matter of experience. *Philosophy & Technology*, *35*, article number 73. https://doi.org/10.1007/s13347-022-00568-6

Gasser, U. (2015). *Interoperability in the digital ecosystem*. Berkman Center Research Publication Series. http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552584

Gasser, U., & Palfrey, J. (2008). *Breaking down digital barriers: When and how ICT interoperability drives innovation*. SSRN. http://dx.doi.org/10.2139/ssrn.1033226

Gawer, A. (2021). Digital platforms' boundaries: The interplay of firm scope, platform sides, and digital interfaces. *Long Range Planning*, *54*(5). https://doi.org/10.1016/j.lrp.2020.102045

Gjesvik, L. (2022). Private infrastructure in weaponized interdependence. *Review of International Political Economy*, *30*(2), 722–746. https://doi.org/10.1080/09692290.2022.2069145

Google Cloud. (2025, March 18). Google + Wiz: Strengthening multicloud security. *Google Cloud*. https://cloud.google.com/blog/products/identity-security/google-announces-agreement-acquire-wiz

Granstrand, O., & Holgersson, M. (2020). Innovation ecosystems: A conceptual review and a new definition. *Technovation*, *91*. https://doi.org/10.1016/j.technovation.2019.102098

Gray, J. E. (2021). The geopolitics of 'platforms': The TikTok challenge. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1557

Gray, J. E., & Tang, W. (2025). The Chinese metaverse: An analysis of China's policy agenda for extended reality (XR). *Policy & Internet*, *17*, e418. https://doi.org/10.1002/poi3.418

Hall, P. A., & Soskice, D. (Eds). (2001). *Varieties of capitalism: The institutional foundations of comparative advantage*. Oxford University Press.

Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital platform ecosystems. *Electronic Markets*, *30*, 87–98. https://doi.org/10.1007/s12525-019-00377-4

Hollister, S. (2023, September 27). Here are the Qualcomm chips that power Meta's Quest 3 and new Ray-Bans. *The Verge*. https://www.theverge.com/2023/9/27/23891035/meta-quest-3-qualcomm-snapdragon-xr2-gen-2-ar1-gen-1

Hoon, C. (2013). Meta-synthesis of qualitative case studies: An approach to theory building. *Organizational Research Methods*, *16*(4), 522–556. https://doi.org/10.1177/1094428113484969

Hou, J. (2025). Building metaverses with (or without) AI: Variegated AI imaginaries in China's national and local metaverse policies. *Asiascape: Digital Asia*, *12*(1–3), 184–216.

Ikenberry, G. J. (2018). The end of liberal international order? *International Affairs*, *94*(1), 7–23. https://doi.org/10.1093/ia/iix241

Kshetri, N. (2026). Privacy and cybersecurity issues facing the metaverse: An analysis of technological and institutional factors. *Telecommunications Policy*, *50*(3), 103140. https://doi.org/10.1016/j.telpol.2025.103140

Lamina1. (2023). *Whitepaper*. Lamina 1. https://assets-global.website-files.com/63fe332d7b9ae4159d741e55/6435ef54d6c2e389be334d99_L1_Whitepaper_2023.pdf

Lawson, A. N., & Herrada, J. (2022). *Fit-for-purpose payment system interoperability: A framework* (FEDS Notes). Board of Governors of the Federal Reserve System. https://doi.org/10.17016/2380-7172.3136

Lee, L. (2025, January 12). Mark Zuckerberg takes another shot at Apple and says it's "squeezing people" for money. *Business Insider*. https://www.businessinsider.com/mark-zuckerberg-meta-apple-feud-joe-rogan-innovation-ecosystem-2025-1

Leswing, K. (2026, January 12). Apple and Google strike AI deal for Siri, Gemini. *News from Google*. https://blog.google/company-news/inside-google/company-announcements/joint-statement-google-apple/

Lowry, P. B., Boh, W. F., Petter, S., & Leimeister, J. M. (2025). Long live the metaverse: Identifying the potential for market disruption and future research. *Journal of Management Information Systems*, *42*(1), 3–38. https://doi.org/10.1080/07421222.2025.2455770

Mann, M., & Daly, A. (2020). Geopolitics, jurisdiction and surveillance. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1501

Markus, M. L., Majchrzak, A., & Gasser, L. (2002). A design theory for systems that support emergent knowledge processes. *MIS Quarterly*, *26*(3), 179–212. https://doi.org/10.2307/4132330

Meta. (2025a, February 24). *Hand and body privacy notice*. Meta. https://www.meta.com/legal/quest/hand-tracking-privacy-notice/

Meta. (2025b, September 5). *Eye tracking privacy notice*. Meta. https://www.meta.com/legal/quest/eye-tracking-privacy-notice/

Moss, S. (2021, December 3). Meta turns to AWS as 'long-term strategic cloud provider' for acquisitions, third-party collaborations, and AI. *Data Center Dynamics*. https://www.datacenterdynamics.com/en/news/metafacebook-turns-to-aws-as-long-term-strategic-cloud-provider-for-acquisitions-third-party-collaborations-and-ai/

Mueller, M. L., & Farhat, K. (2022). Regulation of platform market access by the United States and China: Neo-mercantilism in digital services. *Policy & Internet*, *14*(2), 348–367. https://doi.org/10.1002/poi3.305

Nieborg, D. B., & Poell, T. (2025). Analyzing institutional platform power: Evolving relations of dependence in the mobile digital advertising ecosystem. *New Media & Society*, *27*(4), 1909–1927. https://doi.org/10.1177/14614448251314405

Ortiz-Freuler, J. (2023). The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century. *Global Media and China*, *8*(1), 6–23. https://doi.org/10.1177/20594364221139729

Ortiz-Freuler, J. (2025). Infrastructural power: State strategies for internet control. *Internet Policy Review*, *14*(2). https://doi.org/10.14763/2025.2.2009

Ott, L., Roter, M., Krämer, J., & Ackermann, T. (2026). Enabling competition through standardization: Insights on adversarial standard setting from the EU's interoperability regulation. *Journal of Competition Law & Economics*, 1–45. https://doi.org/10.1093/joclec/nhag023

Palantir Technologies. (2026, March 12). *Palantir and NVIDIA team to deliver sovereign AI operating system reference architecture*. Palantir Technologies. https://investors.palantir.com/news-details/2026/Palantir-and-NVIDIA-Team-to-Deliver-Sovereign-AI-Operating-System-Reference-Architecture/

Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). *Platform revolution: How networked markets are transforming the economy and how to make them work for you*. WW Norton & Company.

Pernin, C. G., O'Mahony, A., Germanovich, G., & Lane, M. (2020). *Chasing multinational interoperability: Benefits, objectives, and strategies* (RR-3068; Research Report). RAND Corporation. https://www.rand.org/pubs/research_reports/RR3068.html

Plantin, J. C., & De Seta, G. (2019). WeChat as infrastructure: The techno-nationalist shaping of Chinese digital platforms. *Chinese Journal of Communication*, *12*(3), 257–273. https://doi.org/10.1080/17544750.2019.1572633

Plantin, J. C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2016). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, *20*(1), 293–310. https://doi.org/10.1177/1461444816661553

Pohle, J., Nanni, R., & Santaniello, M. (2025). Unthinking digital Sovereignty: A critical reflection on origins, objectives, and practices. *Policy & Internet*, *16*(4), 666–671. https://doi.org/10.1002/poi3.437

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Reuters. (2025, November 5). Google's $32 billion deal for Wiz clears DOJ antitrust review, Wiz CEO tells WSJ. *Reuters*. https://www.reuters.com/business/googles-32-billion-deal-wiz-clears-doj-antitrust-review-wiz-ceo-tells-wsj-2025-11-05/

Schmalz, S. (2024). Varieties of digital capitalism and the US–China rivalry: The rise of competing technological spheres. *Critical Sociology*, *51*(4–5), 867–886. https://doi.org/10.1177/08969205241291645

Schöbel, S. M., & Leimeister, J. M. (2023). Metaverse platform ecosystems. *Electronic Markets*, *33*(1), 12. https://doi.org/10.1007/s12525-023-00623-w

Segal, A. (2020). *China's vision for cyber sovereignty and the global governance of cyberspace* (No. 87; NBR Special Report, pp. 85–100). National Bureau of Asian Research. https://www.nbr.org/wp-content/uploads/pdfs/publications/sr87_aug2020.pdf

Segal, A. (2021). Huawei, 5G, and weaponized interdependence. In D. W. Drezner, H. Farrell, & A. L. Newman (Eds), *The uses and abuses of weaponized interdependence* (pp. 143–157). Brookings Institution Press.

Srnicek, N. (2017). *Platform capitalism*. John Wiley & Sons.

Thelen, K. (2018). Regulating Uber: The politics of the platform economy in Europe and the United States. *Perspectives on Politics*, *16*(4), 938–953.

Trendforce. (2024). *Apple's Vision Pro reshapes the VR/MR landscape, driving applications from entertainment to productivity tools, says TrendForce*. Trendforce. https://www.trendforce.com/presscenter/news/20241219-12419.html

Tu, X., & de Castro e Silva, B. (2025). Are we ready for the metaverse? Implications, legal landscape, and recommendations for responsible development. *Digital Society*, *4*(1), article number 9. https://doi.org/10.1007/s44206-025-00163-0

Tusikov, N. (2019). How US-made rules shape internet governance in China. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1408

Tusikov, N. (2021). Internet platforms weaponizing choke points. In D. W. Drezner, H. Farrell, & A. L. Newman (Eds), *The uses and abuses of weaponized interdependence* (pp. 133–148). Brookings Institution Press.

US Securities and Exchange Commission. (2026). *Annual report for the fiscal year ended December 31, 2025* (Form 10-K). US Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1315098/000131509826000024/rblx-20251231.htm

Van Der Vlist, F. N., Helmond, A., Burkhardt, M., & Seitz, T. (2022). API governance: The case of Facebook's evolution. *Social Media + Society*, *8*(2). https://doi.org/10.1177/20563051221086228

Van Der Vlist, F. N., Helmond, A., Dieter, M., & Weltevrede, E. (2024). Super-appification: Conglomeration in the global digital economy. *New Media & Society*, *27*(6), 3314–3337. https://doi.org/10.1177/14614448231223419

Woods, D. (2025). Escaping a weaponized network: China's reaction to the United States escalating technology controls. *Asian Review of Political Economy*, *4*(1), article number 5. https://doi.org/10.1007/s44216-025-00047-7

Wu, E. (2021). *Sovereignty and data localization*. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://live-hksbelfer.pantheonsite.io/sites/default/files/2021-07/SovereigntyLocalization.pdf

Yin, R. K. (2009). *Case study research: Design and methods* (4th edn). Sage Publications.

Published by

Alexander von Humboldt Institute for Internet and Society

CAIS Research for the Digital Age

in cooperation with

CREATe

UOC R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

cnrs centre internet et societe

University of Tartu Johan Skytte Institute of Political Studies