REAL INSTITUTO elcano ROYAL INSTITUTE 25 AÑOS·YEARS

Contestability, innovation, security: resolving the trilemma of digital platform interoperability regulation

Judith Arnal

Elcano Policy Paper

April 2026

Elcano Royal Institute

Global intelligence in Spanish

The Elcano Royal Institute is the leading Spanish think tank in international and strategic studies, and a knowledge centre of European and worldwide renown. Established in 2001 as a private foundation of general interest, our mission is to contribute to drawing up innovative, rigorous and independent responses to global challenges and their governance, and to Spain's role in Europe and the world, in the service of public and private decision-makers and society as a whole.

The organisational structure of the Elcano Royal Institute reflects the main sources of public and private support that enable it to discharge its functions, encouraging an exchange of ideas in a pluralistic and independent environment. Its highest governing body is the Board of Trustees, under the honorary chairmanship of HM King Felipe VI. It also offers a Corporate Partners' Programme.

www.realinstitutoelcano.org

C/ Príncipe de Vergara, 51
28006 Madrid
www.realinstitutoelcano.org

ISSN 2255-5293
Depósito Legal: M-8692-2013

Impreso en Quinteral - Madrid

El papel utilizado en este documento tiene el
certificado del Forest Stewardship Council®

REAL INSTITUTO elcano ROYAL INSTITUTE 25 AÑOS·YEARS

Contestability, innovation, security: resolving the trilemma of digital platform interoperability regulation

Judith Arnal

April 2026

Index

Executive summary

Interoperability sounds like an engineering concern, but it is one of the most consequential questions in modern competition policy. Consider two familiar situations. A consumer who pairs Samsung Galaxy Buds with an iPhone may find that some of the features available with AirPods are not replicated to the same extent across ecosystems; and a Signal user in Europe cannot exchange messages with a contact on WhatsApp, despite both services performing the same function. In each case, the user is trapped inside the gatekeeper's walled garden and switching costs unrelated to product quality sustain the incumbent's market position.

This is why interoperability matters: where it is foreclosed, incumbency advantages compound in ways that resist competitive correction even when challengers offer superior products. The EU responded with the Digital Markets Act (DMA), which through Articles 6(7) and 7 imposes vertical and horizontal interoperability obligations on designated gatekeepers. This regulatory intervention is layered on top of interoperability that gatekeepers already offer voluntarily through exposed APIs and developer programmes, and in some cases through formal request-based processes administered by the platforms themselves. The DMA's distinctive contribution is not the invention of interoperability in digital ecosystems, which largely preceded it, but the imposition of *ex-ante* obligations on designated gatekeepers to provide interoperability at the points where market incentives alone have failed to deliver it. It is the most ambitious *ex-ante* regime enacted anywhere. Yet ambition does not equal coherence.

Interoperability regulation must simultaneously serve three objectives that do not pull uniformly in the same direction: market contestability (reducing lock-in and switching costs); innovation incentives (preserving the appropriability conditions that justify platform investment); and security (protecting closed ecosystems from the attack surfaces that third-party access can create). This is the contestability-innovation-security trilemma, and no architecture resolves it without remainder. The question is whether the DMA navigates the trade-offs intelligently. Three years into implementation, the answer is that it does not.

The DMA's primary-level obligations are simultaneously over-inclusive in scope and underdetermined in normative content: they apply uniformly to every designated gatekeeper without calibration to proved need, while failing to specify the outcome criteria against which compliance should be judged. The result is a structural risk of compliance minimalism at gatekeeper level and, in reaction, a Commission drawn towards prescriptive-in-means implementing acts that risk crystallising specific technical architectures into binding law. The March 2025 Apple specification decision illustrates the vertical dimension: the Commission identified nine specific iOS features that Apple must open to third parties and also prescribed in detail how Apple should run the process it had established in January 2024 through which developers can request access to other features. The concern is that, by fixing today's technical choices in a binding legal decision, the regime may leave little room for those choices to evolve as the underlying technology changes. The November 2025 WhatsApp launch illustrates the horizontal one: Meta shaped the interoperable architecture around its own infrastructure, while Signal and Threema –the services most committed to privacy-preserving design– were structurally excluded. The security derogation meant to prevent this outcome delivered its inverse.

The UK and Japan have made architecturally distinct choices within the same policy window. The UK's Digital Markets, Competition and Consumers Act relies on a collaborative, firm-specific conduct-requirement process, with proportionality embedded upstream and technological neutrality preserved throughout. Japan is a particularly instructive case: its Mobile Software Competition Act drew openly on the DMA as a template, yet departed from it on the points that have proved most problematic, adopting a functional equivalence standard and commitment procedures that soften the reactive character of regulatory intervention. Neither regime achieves full coherence, but both illuminate trade-offs the DMA has not.

Three reforms follow. First, Articles 6(7) and 7 should be reformulated to specify outcome criteria –timeliness, technical completeness and absence of unjustified conditions– without prescribing technical means. Secondly, interoperability should be activated on a demand-driven basis, through the gatekeeper's own request process, with prescriptive regulatory specification reserved as a residual mechanism where that process demonstrably fails to deliver. And, third, an independent European digital authority should be entrusted with monitoring outcome criteria, evaluating security claims with genuine technical expertise, and insulating enforcement from the geopolitical pressures the Commission cannot structurally resist.

The DMA review cycle, and the jurisdictions now using its architecture as a template, offer a time-limited opportunity to internalise these lessons before they harden into a second generation of frameworks. This Policy Paper develops the diagnosis in full, grounds it in the implementation record of the DMA's interoperability regime, compares it against the regulatory architectures of the UK and Japan, and sets out the three reforms in detail.

1. Introduction

The regulation of digital platform interoperability has emerged as one of the most consequential and technically demanding challenges in contemporary competition policy. The premise is well-established: in markets characterised by strong network effects, data-driven barriers to entry, and ecosystem dynamics that allow dominant platforms to extend market power into adjacent services, the ability of third parties to access, connect to and build upon gatekeeper infrastructure is not merely a matter of commercial convenience but a structural determinant of contestability. Where interoperability is foreclosed, incumbency advantages compound in ways that resist competitive correction even where challengers offer superior products, and the self-reinforcing character of concentration produces market structures that *ex-post* enforcement instruments are poorly suited to address. The policy response across major jurisdictions has accordingly shifted toward *ex-ante* regulatory frameworks that impose affirmative interoperability obligations on designated gatekeepers as a condition of market participation.

The Digital Markets Act (Regulation (EU) 2022/1925) is the most ambitious instance of this approach. Through Articles 6(7) and 7 the DMA establishes vertical and horizontal interoperability obligations applicable to designated gatekeepers across their core platform services, signalling a departure from the reactive, effects-based logic of competition law enforcement towards prospective, structural intervention. In the three years since its entry into force, the DMA's interoperability regime has accumulated a substantial implementation record that now permits a systematic assessment of whether the regulatory architecture adopted by the legislature is fit for the objectives it was designed to serve.

This paper argues that it is not, and that the failure is structural rather than incidental. The DMA's interoperability provisions suffer from a design defect that operates across both normative levels of the regime simultaneously: at the primary level, the obligations are over-inclusive in scope and normatively underdetermined in content, providing insufficient orientation to gatekeepers seeking to comply and insufficient analytical structure to constrain the Commission's specification discretion; at the secondary level, the corrective

mechanism available under Article 8(2) is reactive, unilateral and prescriptive in means, producing feature-specific implementing acts that crystallise particular technical architectures into binding legal requirements at a given moment in time. The combination generates a regulatory dynamic in which compliance minimalism at the gatekeeper level provokes prescriptive specification at the Commission level, with the result that the regime reproduces the characteristic weaknesses of both rule-based and principles-based regulatory architectures without capturing the advantages of either.

The analysis of this failure is organised around a trilemma that constitutes the paper's central analytical contribution. Interoperability regulation must simultaneously serve the objective of market contestability, by reducing the switching costs and lock-in effects that sustain incumbency advantages derived from network externalities; preserve incentives for platform-level innovation, by maintaining the appropriability conditions that justify irreversible investment in new features and architectures; and respect the security constraints that arise from opening closed ecosystems to third-party access. These three objectives do not pull uniformly in the same direction, and no regulatory architecture resolves the tension among them fully: every design generates trade-offs that persist. The analytical value of the trilemma lies not in the identification of an optimal equilibrium –none exists– but in providing a systematic framework for assessing the trade-offs that any given regulatory design necessarily produces, and for identifying where the DMA's architecture fails most consequentially.

Two case studies ground the trilemma analysis in the specifics of the DMA's implementation experience. In the vertical dimension, the specification proceedings against Apple (DMA.100203 and DMA.100204), culminating in the March 2025 implementing acts identifying nine iOS connectivity features subject to mandatory third-party access and prescribing the detailed means by which Apple must administer its request-based interoperability process, illustrate a regime of comprehensive means-prescription in which the regulator specifies both the substance of interoperability and the procedure by which further access is sought, rather than defining the outcome criteria that the gatekeeper's process must satisfy and intervening proportionately where it fails to meet them. In the horizontal dimension, the launch of WhatsApp interoperability in November 2025 pursuant to Article 7 illustrates a different and analytically more troubling failure: mandated cross-platform messaging interoperability in an end-to-end encrypted environment produces a configuration in which the dominant incumbent shapes the interoperability architecture on terms that suit its own technical infrastructure, with the effect that providers operating under more demanding security models are structurally excluded from participation. The security derogation clause of Article 7(9) was intended to protect against precisely this outcome; the implementation record suggests it has failed to do so.

The paper's comparative analysis examines how the UK and Japan have addressed the same regulatory challenge within the same policy window, making architecturally distinct choices that generate observable variation against the dimensions of the trilemma. The Digital Markets, Competition and Consumers Act 2024 (DMCC) delegates entirely to a collaborative, firm-specific secondary process, embedding proportionality upstream and preserving technological neutrality at both normative levels, at some cost to the immediacy of contestability protection. Japan's Act on Promotion of Competition for Specified Smartphone Software (MSCA) adopts a functional equivalence standard at the primary level –technologically neutral as to means whilst more normatively determinate than the DMA's parity standard– and introduces commitment procedures that partly mitigate the reactive character of its secondary level. Neither jurisdiction achieves full coherence across the trilemma; each illuminates a different set of trade-offs, and the diffusion of these models to jurisdictions still designing their frameworks –Australia, India, South Korea– makes the choice of architecture a question of immediate practical relevance beyond the three enacted regimes.

The analysis draws on three complementary methodological approaches. The theoretical framework of Section 2 is grounded in the economics of regulation and two-sided market theory, deploying the error-cost framework and the literature on regulatory design to derive a taxonomy of interoperability architectures and their expected welfare implications. The assessment of the DMA in Section 3 combines doctrinal analysis of the primary and secondary legislative instruments with an examination of the Commission's specification decisions, BEREC opinions, and the available implementation record from Apple and Meta; it is necessarily bounded by the recentness of the events under analysis, and assessments based on proceedings concluded in 2025 and early 2026 should be read with that temporal constraint in mind. The comparative analysis of Section 4 applies a structured comparison across two analytical axes –the degree of normative determinacy at the primary level and the character of the secondary specification process– selecting the UK and Japan as the comparators on the ground that both have enacted dedicated *ex-ante* digital platform legislation within the same policy cycle as the DMA, making the comparison temporally coherent and the variation in architectural choices analytically motivated rather than incidental. Australia, India and South Korea are examined as diffusion cases rather than primary comparators: their frameworks remain at legislative design stage, and their analytical value lies in the choices they face rather than the implementation experience they have generated.

The paper concludes with three normative proposals addressed to the DMA's review cycle and to the wider community of jurisdictions drawing on its architecture as a template. The first concerns normative determinacy at the primary level: Articles 6(7) and 7 should be reformulated to specify outcome criteria without prescribing those means. The second concerns the character of the secondary level: the regulatory authority should define the outcome

criteria that the gatekeeper's request-based process must satisfy, rather than prescribing comprehensively both the substance of interoperability and the procedural means by which it is administered, with collaborative specification proceedings reserved as a residual mechanism where the process demonstrably fails to meet those criteria. The third concerns institutional capacity: both proposals presuppose a regulatory authority with the technical expertise, institutional continuity, and structural independence to discharge the specification and enforcement functions they require –capabilities that the Commission's current architecture does not consistently possess and that an independent European digital authority, modelled on the ESMA precedent and delimited by the Meroni doctrine, would be better positioned to provide–.

The paper proceeds as follows. Section 2 develops the theoretical framework, establishing the contestability-innovation-security trilemma and the taxonomy of regulatory architectures against which the DMA and its comparators are assessed. Section 3 analyses the DMA's interoperability regime and its implementation experience across both dimensions. Section 4 examines the regulatory architectures of the UK and Japan, including the emerging diffusion of these models to other jurisdictions. Section 5 sets out the normative proposals and section 6 the conclusions.

2. Theoretical framework

2.1. Vertical and horizontal interoperability: a conceptual distinction

Interoperability denotes the ability of distinct systems to exchange information and to make productive use of the information so exchanged. In digital platform markets, a foundational analytical distinction can be drawn between two structurally different forms of interoperability.

'Vertical interoperability' concerns access to functionalities within a gatekeeper's own ecosystem, including operating system features and hardware interfaces, and addresses the risk that a dominant platform forecloses competition by restricting third-party access to the infrastructure on which complementary services depend. Examples include a third-party smartwatch manufacturer seeking access to the NFC and Bluetooth protocols controlled by a mobile operating system, or a third-party digital wallet provider seeking NFC access equivalent to that available to the gatekeeper's own payment service.

'Horizontal interoperability' concerns the capacity of users to interact across competing platforms offering equivalent services, most notably in interpersonal communications markets, where network effects are particularly strong, and addresses the risk that incumbency advantages derived from network size become self-reinforcing barriers to entry (Kerber & Schweitzer, 2017). Examples include the ability of a user on a smaller messaging application to send messages to a contact on WhatsApp without both parties being on the same platform, or a user switching social networks without losing the ability to communicate with contacts who remain on the incumbent service.

These two forms of interoperability are analytically distinct, give rise to different regulatory challenges and, as Section 3 demonstrates, are addressed by the Digital Markets Act through structurally different legal instruments.

2.2. Interoperability and market contestability

The primary economic rationale for mandating interoperability in digital platform markets derives from the contestability effects it generates. Interoperability reduces switching costs and lock-in effects that sustain incumbency advantages derived from network externalities: where the value of a service to any given user increases with the number of other users on the same network, incumbent platforms enjoy a structural competitive advantage that is largely independent of productive efficiency, and market dynamics tend towards tipping, producing concentrated structures that resist competitive entry even where challengers offer superior products (Katz & Shapiro, 1985; Farrell & Saloner, 1985). More recent contributions have emphasised that incumbency advantages in digital markets are further reinforced by data-driven network effects, whereby the accumulation of behavioural data improves algorithmic performance in ways that compound over time, and by ecosystem dynamics in which control over a core platform enables the extension of market power into adjacent services (Crémer, de Montjoye & Schweitzer, 2019; Jacobides, Cennamo & Gawer, 2018).

The application of two-sided market theory introduces, however, an important qualification directly relevant to the design of interoperability obligations. As Rochet & Tirole (2003) established, platforms operating across two distinct user groups, such as end-users and application developers, or consumers and business users, internalise cross-group externalities and set price and quality structures accordingly. An interoperability obligation imposed on one side of the platform does not produce neutral effects on the other. Compulsory access to operating system APIs by third-party hardware manufacturers, for example, may reduce the platform's capacity to sustain investment in the consumer-facing features that generate the installed base on which third-party developers depend.

The welfare effects of interoperability mandates cannot therefore be assessed by reference to static market structure alone: the dynamic implications for incentives to invest across both sides of the ecosystem must be incorporated into the analysis. Where interoperability is asymmetric –requiring the incumbent to bear the costs of integration whilst allowing entrants to free-ride on the incumbent's installed base and infrastructure investment– the resulting competitive dynamics may be distorted in ways that reduce total welfare even as they reduce market concentration (Armstrong, 2006).

Hence, the design of interoperability obligations must attend not only to the static contestability objective but also to the dynamic effects on the competitive structure of the ecosystem as a whole. This distinction between static and dynamic contestability provides one of the key analytical bridges to the innovation effects examined in the following section.

2.3. Interoperability and innovation incentives

The relationship between interoperability mandates and innovation incentives is analytically distinct from the contestability effects examined above, and has generated a separate and sometimes conflicting body of theoretical literature. The central tension arises from the interaction between two well-established mechanisms linking market structure to innovation.

The Schumpeterian tradition emphasises the role of market power in sustaining incentives for long-term, irreversible investment in new products and technologies: the prospect of appropriating supernormal profits provides the return that justifies risky expenditure on research and development (Schumpeter, 1942). On this account, regulatory interventions that erode market power, including interoperability mandates that reduce switching costs and facilitate entry, may weaken the appropriability conditions that sustain innovation incentives, particularly for platform-level investment that benefits the ecosystem as a whole but cannot be easily monetised once third-party access is compelled.

Arrow (1962) offered the contrary insight: an entrenched monopolist faces weaker incentives to innovate than a competitive challenger, since any new product merely cannibalises the monopolist's existing rents. Subsequent empirical work has reconciled these positions, finding that the relationship between competition and innovation follows an inverted-U pattern, with innovation maximised at intermediate levels of competitive pressure (Aghion *et al.*, 2005).

The implication for interoperability regulation is not a blanket conclusion in either direction, but a calibration problem. Applied specifically to the 'prescriptiveness' of interoperability obligations, the error-cost framework developed by Easterbrook (1984) and extended to dynamic markets by Manne & Wright (2010) provides a useful analytical lens. The framework directs attention to the relative social costs of different types of regulatory error under uncertainty. Applied to interoperability regulation, a Type I error, ie, an over-prescriptive obligation that inadvertently constrains procompetitive investment or product differentiation, risks entrenching a suboptimal technical standard in legal requirements. A Type II error, ie, an insufficiently specific obligation that

permits a gatekeeper to frustrate contestability through technical obfuscation or compliance minimalism, allows incumbency advantages to persist. The error-cost framework does not resolve this trade-off, but it directs attention to two features of regulatory design that bear directly on prescriptiveness: the 'reversibility' of the chosen instrument, and the mechanisms through which compliance is assessed and updated over time.

The application of this framework to *ex-ante* platform regulation requires an important qualification. Easterbrook's original argument assumed that market self-correction mechanisms, ie, entry and competitive pressure, would mitigate Type II errors over time, making under-intervention relatively less costly in the long run. In digital platform markets characterised by strong network effects and data-driven barriers to entry, self-correction may operate too slowly to be policy-relevant (Crémer *et al.*, 2019). This asymmetry modifies the error-cost argument without overturning it: the appropriate response is not the abandonment of *ex-ante* obligations, but the design of regulatory instruments that minimise the lock-in costs of Type I errors, particularly the risk of crystallising a specific technical architecture into binding legal requirements, while maintaining sufficient regulatory pressure to prevent gatekeepers from exploiting compliance ambiguity.

2.4. Security as a regulatory constraint

Security considerations occupy a structurally distinct position in the analysis of interoperability regulation. Unlike contestability and innovation, which represent objectives that interoperability mandates seek to advance, albeit with different and sometimes conflicting implications, security operates primarily as a 'constraint' on the design and scope of interoperability obligations. This distinction has important implications for how security concerns should be incorporated into the regulatory framework.

The extension of interoperability access to third parties introduces risks that are not present in relatively closed ecosystems: vulnerabilities in third-party implementations may expose users of the incumbent platform to security threats; the requirement to maintain end-to-end encryption across interoperable services creates cryptographic complexity that may be difficult to manage without compromising the integrity of either system; and the obligation to provide access to low-level hardware and software features, such as NFC controllers or Bluetooth stacks, may, if poorly specified, create attack surfaces that could be exploited at scale. These are not hypothetical concerns, as Section 3 demonstrates through the implementation experience of both the vertical and horizontal dimensions of the DMA's interoperability regime.

At the same time, security justifications can function as a strategic instrument through which gatekeepers resist compliance with interoperability obligations by invoking risks that are either overstated or addressable through less restrictive means. The DMA's response to this tension, permitting strictly necessary and proportionate derogations, duly justified by the gatekeeper, is a principles-based standard embedded within an otherwise prescriptive regime. Its effectiveness depends critically on the capacity of the Commission to evaluate the technical merits of security claims with sufficient expertise and in sufficient time to prevent security justifications from becoming a source of systemic delay.

2.5. Synthesis: the architecture of the norm

The preceding analysis establishes three analytically distinct dimensions along which the welfare effects of interoperability regulation must be assessed: market contestability, innovation incentives and security. These dimensions do not pull uniformly in the same direction, and the regulatory design challenge, particularly the choice of regulatory architecture, must be evaluated against all three simultaneously.

The literature on regulatory design distinguishes broadly between prescriptive and principles-based approaches to *ex-ante* regulation (Baldwin, Cave & Lodge, 2012; Black, 2008). Building on this distinction, and extending it to the specific context of interoperability obligations in digital platform markets, this paper proposes a taxonomy of three regulatory architectures, each carrying distinct implications for the contestability-innovation-security trilemma.

A 'prescriptive' *ex-ante* norm specifies in advance the precise conduct required of regulated entities: the APIs that must be exposed, the protocols that must be adopted, the technical features that must be made accessible and the timelines within which compliance must be achieved. Prescriptive obligations offer legal certainty and reduce the scope for strategic non-compliance, thereby serving the contestability objective. They carry a characteristic risk, however: 'regulatory lock-in', whereby a particular technical architecture is crystallised into legal requirements at a point in time, such that subsequent innovation involving departures from that architecture faces a structural compliance burden (Lemley & McGowan, 1998). In rapidly evolving ecosystems, prescriptive obligations may also reduce incentives to invest in new platform features that may become subject to mandatory third-party access and may leave security constraints inadequately addressed by the generality of the prescribed standard.

A 'principles-based' *ex-ante* norm articulates the objectives and criteria that regulated conduct must satisfy, such as effectiveness, timeliness, proportionality and non-discrimination, without specifying the technical means of achieving them. Principles-based obligations preserve flexibility for regulated entities to adapt their compliance approach to evolving technological conditions, reducing the risk of regulatory lock-in and creating space for security considerations to be addressed on a case-by-case basis. They do so at some cost to legal certainty and to the practical ability of third parties to assess and contest compliance. Their effectiveness depends heavily on the institutional capacity of the regulatory authority to engage with complex technical questions in real time (Black, 2008; Baldwin, Cave & Lodge, 2012).

A 'procedural' *ex-ante* framework occupies a distinct position in this taxonomy. Rather than specifying either the substantive outcome or the technical means, procedural obligations require regulated entities to follow prescribed processes, such as structured engagement with third-party requesters, transparent documentation of implementation decisions, defined timelines for responding to interoperability requests and accessible dispute resolution mechanisms. Procedural obligations reduce the information asymmetry between regulator and regulated entity by generating a structured, auditable record of compliance decisions, without requiring the regulator to pre-specify the technical content of those decisions. They are most valuable precisely where the pace of technological change makes substantive pre-specification unreliable and where security justifications require iterative technical evaluation rather than blanket rules.

A critical analytical point developed further in Sections 3 and 4, is that in practice interoperability regimes operate across multiple normative levels: a primary legislative instrument may establish principles-based or outcome-oriented obligations, whilst secondary implementing measures issued by the regulatory authority specify the technical means of compliance in binding detail. The overall character of the regime, and its implications for the contestability-innovation-security trilemma, cannot be assessed by reference to the primary instrument alone but must account for the full normative architecture, including the implementing measures that give it technical content. Where secondary measures are prescriptive in means, they risk compromising technological neutrality even where the primary instrument is technologically agnostic, and they reproduce the lock-in risk at a more granular level.

The taxonomy developed above can be systematised against the three objectives the regime must simultaneously serve. Figure 1 maps the four architectures identified in the preceding analysis –including the hybrid configuration that characterises the DMA as enacted– against the contestability-innovation-security trilemma. The Figure serves as an analytical reference point for the assessment of the DMA's implementation experience in Section 3 and the comparative analysis of the DMCC and MSCA in Section 4.

Figure 1.

Taxonomy of interoperability regulatory architectures: trilemma implications

Architecture	Defining features	Contestability	Innovation incentives	Security
Prescriptive *ex-ante*	Specifies in advance exact APIs, protocols and features to be exposed; fixed timelines for compliance	Strong Legal certainty; minimal scope for strategic non-compliance	Weak Regulatory lock-in; chills investment in new platform features subject to immediate mandatory access	Mixed Prescribed standards may become technically outdated; generalised requirements may inadvertently create attack surfaces
Principles-based *ex-ante*	Specifies objectives and criteria (effectiveness, non-discrimination, proportionality); technical means left to regulated entity	Moderate Flexibility preserved; effectiveness depends heavily on regulator's technical capacity to assess compliance	Strong Avoids lock-in; accommodates technological evolution; preserves appropriability conditions	Strong Case-by-case evaluation of security constraints; derogations assessed on their technical merits
Procedural *ex-ante*	Prescribes processes (structured engagement, documentation, timelines and dispute resolution) rather than substantive outcome or technical means	Moderate Structured record enables compliance assessment; immediacy depends on process speed	Strong Reduces information asymmetry without pre-specifying technical content; preserves adaptation latitude	Strong Iterative technical evaluation; security justifications auditable through structured process record
Over-inclusive primary + prescriptive secondary *DMA as enacted*	Broad primary-level standard corrected by reactive implementing acts that prescribe both the substance of interoperability (specific features) and the detailed procedural means by which the gatekeeper must administer its request-based process	Contested Immediate obligations at designation; compliance minimalism incentivised by normative underdetermination	Doubly constrained Primary standard chills investment; secondary implementing acts crystallise both technical architecture and procedural design at point of specification	Weak Security or integrity derogations create contestable space for strategic delay; evaluation demands exceed current institutional capacity

Source: the author.

The final row of Figure 1 identifies the specific configuration that the analysis of Section 3 demonstrates the DMA has produced in practice: a regime that combines the weaknesses of prescriptive and principles-based architectures without capturing the advantages of either. The implication is that interoperability by regulatory design, ie, the imposition of broad, uniform access obligations triggered by designation, is not the optimal architecture. The *ex-ante* obligation should instead define outcome criteria that the gatekeeper's request-based process must satisfy, including transparency, reasonable timelines and non-discriminatory evaluation, whilst leaving the design of the process to the gatekeeper. The regulatory authority's role is to assess whether the process delivers effective interoperability against those criteria and to intervene proportionately where it does not, rather than to prescribe the process's design *ex-ante*. As the comparative analysis of Section 4 confirms, regimes that distinguish between outcome prescription and means prescription generate more coherent outcomes across the trilemma.

3. The DMA interoperability regime: architecture, constitutive tensions and implications for the trilemma

3.1. Regulatory logic and the design of interoperability obligations

The Digital Markets Act (Regulation (EU) 2022/1925) establishes an *ex-ante* regulatory framework targeting large digital platforms designated as gatekeepers on the basis of their structural market position and intermediation power. The legislative choice to shift from *ex-post* competition law enforcement to prospective obligations reflects a judgement that the structural features of digital platform markets make competitive self-correction insufficiently reliable to serve as the primary regulatory mechanism (Crémer *et al.*, 2019; Larouche & de Streel, 2021).

Within this framework, interoperability operates as a central instrument for restoring the contestability that gatekeeper incumbency has foreclosed. The Regulation operationalises this objective through two structurally distinct obligations whose analytical difference, as established in Section 2.1, maps onto structurally different forms of competitive harm.

Article 6(7) governs vertical interoperability, requiring gatekeepers to provide free and effective interoperability with the same hardware and software features, including NFC chips, Bluetooth connectivity protocols, Wi-Fi peer-to-peer functions, and device pairing interfaces, as are available to the gatekeeper's own services. The standard is one of parity: third parties must receive the same access as the gatekeeper affords its own vertically integrated services.

Article 7 governs horizontal interoperability, requiring gatekeepers providing number-independent interpersonal communications services to enable third-party providers to interoperate with the basic functionalities of the gatekeeper's service on a staged implementation timeline extending to four years after designation.

Both provisions share a common structural defect at the primary level: they are simultaneously over-inclusive in scope and underdetermined in normative content. As a consequence, both generate a reactive and prescriptive secondary level that compounds rather than resolves it, though the way in which this plays out, and its implications for the trilemma, differs between the vertical and horizontal dimensions in ways that the following sections examine.

3.2. The constitutive tension at the primary level: over-inclusion and normative underdetermination

The most analytically significant structural weakness of the DMA's interoperability regime does not lie exclusively at the secondary level of implementing acts, though the secondary level compounds it severely, but in the design of the primary-level obligations themselves. Articles 6(7) and 7 are simultaneously over-inclusive in their scope and underdetermined in their normative content, a combination that generates predictable and mutually reinforcing difficulties across all dimensions of the trilemma, in both the vertical and horizontal dimensions of the regime.

The over-inclusion is structural. Both provisions apply uniformly to all designated gatekeepers, without calibration to the specific competitive dynamics of the ecosystem in question, the market position of third-party requesters relative to the gatekeeper, or the degree to which the foreclosure problem that motivates each obligation is actually present in the particular context. The contrast with the EU telecoms regime is instructive: under the Electronic Communications Code, national regulatory authorities are required to impose obligations that are proportionate and constitute the least intrusive

means of addressing a specifically identified market failure (Ibáñez Colomo, 2021). The DMA imposes no equivalent proportionality requirement at the stage of obligation design.

This design places the burden of compliance definition on the gatekeeper, a structural feature that creates perverse incentives in both directions. On one hand, the gatekeeper facing a broadly framed obligation with uncertain boundaries has an incentive to adopt the most restrictive interpretation compatible with the obligation's text, invoking security or technical integrity justifications at the margins to resist broader access (Lundqvist, 2024). On the other hand, the absence of a primary-level proportionality constraint means that, once the Commission opens specification proceedings, the resulting implementing act is not required to identify the least intrusive means of achieving the regulatory objective at the point of design. This distinguishes the DMA from both the EU telecoms regime, where proportionality operates upstream as a substantive limit on the regulator's choice of obligation, and from competition law *ex-post* remedies, where the Commission cannot impose measures going beyond what is necessary to bring the infringement to an end. Proportionality under the DMA enters the analysis only *ex-post*, as a parameter of judicial review, leaving the Commission with substantially broader prescriptive discretion at the specification stage than either framework would permit (Ibáñez Colomo, 2021).

The underdetermination problem is equally present in both obligations, though it manifests differently. In the vertical dimension, the parity standard of Article 6(7) does not articulate what parity requires as a regulatory outcome in the context of features architecturally designed for integrated rather than third-party use: it neither defines the criteria by which parity is to be assessed, nor identifies the boundaries within which the secondary level may legitimately specify the means of compliance. In the horizontal dimension, Article 7 does not establish the outcome criteria against which competing technical architectures for cross-platform messaging interoperability are to be evaluated, leaving unresolved not the technical means, which appropriately belong to the secondary level, but the normative benchmarks by which any proposed means must be judged (Blessing & Anderson, 2023). In both cases, the result is an obligation that provides insufficient normative orientation to gatekeepers seeking to comply and insufficient analytical structure to constrain the Commission's specification discretion. The parliamentary process that produced the DMA's final text made both defects worse simultaneously: by broadening the scope of the obligations beyond the Commission's 2020 proposal without supplying the outcome criteria and evaluative benchmarks that would have made that broader scope normatively governable, it generated obligations that are more ambitious in reach than the original design and less actionable in practice than a coherent principles-based regime –combining the coverage of the former with the indeterminacy of the latter, and the advantages of neither (Lundqvist, 2024)–.

The implications for the trilemma are consequential and shared across both dimensions. For contestability, the underdetermination of the primary level creates a structural opportunity for compliance minimalism: gatekeepers facing broadly framed obligations have an incentive to adopt compliance approaches that are formally defensible under the applicable standard whilst substantively limiting the access that third parties can extract (Ribera Martínez, 2025). For innovation, the over-inclusive, uniform application of both obligations to all features within their respective scopes creates a chilling effect on platform-level investment that operates regardless of whether the feature in question is relevant to the competitive harm the obligation seeks to address (Larouche & de Streel, 2021). For security, the primary-level derogation clauses[1] –permitting strictly necessary and proportionate measures– provide a standard whose interpretation depends entirely on the Commission's capacity to evaluate compliance with technically complex obligations –a capacity required not only for the adjudication of security claims but more broadly for the assessment of whether measures adopted by gatekeepers effectively achieve the regulatory outcomes the primary-level obligations require–. The way in which these shared consequences play out in practice differs, however, between the vertical and horizontal dimensions, and that difference is the subject of the next two sections.

3.3. The vertical dimension: reactive specification and the lock-in problem

In the vertical dimension, the primary level's underdetermination is corrected, if at all, through the Article 8(2) mechanism, which empowers the Commission to issue implementing acts specifying the measures a gatekeeper must implement to achieve effective compliance with Article 6(7). The secondary level is best understood not as an organic complement to the primary-level obligation but as a structural corrective to its indeterminacy. This reframing carries important analytical consequences: it explains the reactive, unilateral and technically prescriptive character of specification proceedings, and it identifies the systemic lock-in risk that the two-level architecture displaces rather than eliminates.

1 The Article 6(7) safeguard is textually formulated as protection of the 'integrity' of the operating system and software features; Article 7(9) expressly refers to 'security' and end-to-end encryption. This paper uses 'security' throughout as an analytical category encompassing both textual formulations –integrity-based and security-based– as well as the cryptographic, attack-surface and operational-continuity considerations that gatekeepers in practice invoke under both derogations.

The case of Apple (DMA.100203) provides the most fully developed illustration. Specification proceedings were opened in September 2024, not proactively but in response to the Commission's assessment that Apple's compliance measures following its September 2023 designation were insufficient to achieve effective interoperability under Article 6(7). The proceedings, which included a public consultation in December 2024 and extensive technical engagement with Apple and third-party developers, resulted in a decision adopted in March 2025 establishing detailed implementation timelines for nine specific iOS connectivity features, calibrated to Apple's development cycle and staged across three tranches: an initial set of measures required by end-2025; a principal tranche by 1 June 2026; and a residual tranche by end-2026, aligned with iOS 27, with a narrow subset extended to 1 June 2027. Whilst the process superficially resembles collaborative regulatory dialogue, the output is a legally binding, unilateral implementing act to which Apple objected and against which it subsequently initiated litigation. The procedural appearance of flexibility through staged timelines, calibration to development cycles does not alter the substantive character of the instrument: a prescriptive-in-means decision that fixes specific technical standards at a particular point in time (European Commission, 2025).

The March 2025 proceedings produced, alongside the implementing act specifying nine connectivity features (DMA.100203), a parallel decision (DMA.100204) specifying measures to improve the request-based interoperability process Apple had established for developers under Article 6(7). The analytical significance of this second decision has been insufficiently examined. Apple had established a process through which developers could request access to iOS and iPadOS features, with evaluation criteria and development timelines. The Commission's decision to regulate that process comprehensively –imposing enhanced documentation obligations, structured timelines, a conciliation mechanism and annual reporting requirements– may have been motivated by identified deficiencies in the process as originally designed. However, the character of the regulatory response raises a question that is directly relevant to the trilemma. If the request-based process was underperforming, the proportionate regulatory response would be to identify and correct the specific deficiencies, eg, excessive delays, opaque rejection criteria and inadequate technical documentation, rather than to prescribe the entirety of the process through a binding specification decision. DMA.100204 follows the same prescriptive logic as DMA.100203, applied not to the features themselves but to the process by which access to further features is requested and evaluated. The result is a regime in which both the substance and the procedure of interoperability are specified top-down, leaving limited space for a genuinely demand-driven model in which the gatekeeper's process operates as the primary channel and regulatory intervention is reserved for evidenced failures.

The lock-in risk operates at two levels simultaneously. At the level of the specific decision, the prescriptive channel (DMA.100203) operates in its classical form: features not among the nine specified are excluded, and each new category requires new proceedings. The parallel decision (DMA.100204) does not resolve this problem, since it merely prescribes, in equally binding and comprehensive terms, how the gatekeeper must administer its own request-based process, rather than allowing that process to operate as a genuinely demand-driven channel subject to proportionate regulatory oversight. Neither decision achieves what the trilemma analysis suggests is optimal: a model in which the *ex-ante* obligation requires the gatekeeper to maintain a functioning request-based process and to respond to legitimate third-party requests within defined parameters, whilst the regulatory authority exercises proportionate oversight over the process's effectiveness rather than prescribing comprehensively both the substance of interoperability and the procedure by which it is requested and evaluated. At the level of the broader regulatory architecture, the accumulation of feature-specific implementing acts under the prescriptive channel progressively crystallises the technical architecture of a gatekeeper's ecosystem, as it exists at the moment of specification, into binding legal requirements. The lock-in risk identified in Section 2.5 is not eliminated by the two-level design; it is displaced to the secondary level, where it is less visible in the legislative text but no less real in its consequences for technological neutrality and dynamic innovation incentives.

For the innovation dimension of the trilemma, this creates a compounding effect. In the prescriptive channel, the primary-level parity standard chills investment in new platform features, since any functionality developed by the gatekeeper for its own services must immediately be made available to third parties on equivalent terms. The secondary-level specification process then fixes the technical implementation of that access at a particular moment, removing the gatekeeper's latitude to evolve the technical means of compliance as the underlying technology develops. The result is a regulatory environment in which investment in new platform architecture faces a double constraint: the immediate appropriability concern at the primary level and the crystallisation risk at the secondary level. In the process channel, the means-prescription of DMA.100204 compounds this effect: by fixing the procedural architecture through which further access is sought, it reduces the gatekeeper's capacity to adapt the process to evolving technological and market conditions. Rules alone are insufficient in sectors evolving as rapidly as digital platform markets; they require complementary processes responsive to actual market needs rather than regulatory proceedings activated in response to identified compliance gaps (Larouche & de Streel, 2021).

For the security dimension, the vertical context generates a distinct but equally significant problem. The features subject to Article 6(7) –NFC controllers, Bluetooth stacks, Wi-Fi peer-to-peer protocols– are low-level hardware and software functionalities architecturally designed as closed components of an

integrated system. Opening them to third-party access through prescriptive implementing acts that mandate access across the board creates attack surfaces that the original security architecture of the operating system was not designed to accommodate, introducing entry points for malicious actors that are structurally different from, and more difficult to contain than, those arising from application-level API access (CEPA, 2025). The Apple specification proceedings illustrate the problem: a significant portion of Apple's contestation of the March 2025 decision rested on precisely these grounds, arguing that the required access to NFC and related low-level features would compromise the integrity of iOS's security architecture in ways that the derogation clause of Article 6(7), interpreted narrowly by the Commission, did not adequately accommodate. Whether these claims were technically well-founded or functioned primarily as instruments of strategic delay cannot be determined from the public record alone –and that epistemic uncertainty is itself a structural feature of the problem–. The derogation clause creates a space of contestable security justification whose boundaries cannot be drawn without technical expertise and real-time evaluative capacity that the Commission's current enforcement infrastructure only partially possesses.

3.4. The horizontal dimension: the security paradox of mandated interoperability

The horizontal dimension of the DMA's interoperability regime shares the same primary-level defects –over-inclusion and normative underdetermination– as the vertical dimension analysed above. The Article 7 obligation applies uniformly to all designated messaging gatekeepers without calibration to the specific competitive harm present in each case, and it leaves unresolved the foundational technical questions that any serious implementation of cross-platform messaging interoperability must address. The secondary level corrects this indeterminacy only partially, through the BEREC consultation process and the Commission's review of reference offers, without the binding specificity of the Article 8(2) implementing acts available in the vertical dimension. What distinguishes the horizontal case analytically is not the regulatory architecture, which reproduces the same structural tensions, but the specific way in which those tensions interact with the cryptographic architecture of end-to-end encrypted communications services to produce an outcome that is the inverse of the security objective the derogation clause of Article 7(9) was designed to protect.

The legislative history of Article 7 is itself revealing of the underdetermination problem. The original Commission proposal did not include a horizontal interoperability obligation for messaging services; the provision was

introduced during parliamentary negotiations, without the technical specification that would have been required to assess its implications for end-to-end encryption, and over the reservations of Commission officials who had doubts about its feasibility (Lundqvist, 2024). The security carve-out of Article 7(9) –permitting strictly necessary and proportionate measures including the maintenance of end-to-end encryption– is both essential to the provision's legal credibility and deeply uncertain in its operational content.

Making end-to-end encrypted messaging services interoperable raises unresolved technical problems at every layer of the system. How users are identified and authenticated across platforms, how encryption keys are managed without a shared identity infrastructure, how contacts on one service are discoverable to users on another without generating metadata exposures, and how spam and abuse are moderated across systems with incompatible content policies: none of these questions has a settled answer (Blessing & Anderson, 2023). The root difficulty is structural. End-to-end encrypted messaging systems were designed as closed, centralised architectures; making them interoperable requires decisions about key federation and cross-platform trust that cannot be resolved simply by preserving encryption at the level of individual messages.

The WhatsApp case illustrates how these constraints translate into paradoxical regulatory outcomes. When Meta launched Article 7 interoperability for European users in November 2025, it did so through a client-to-server-to-client architecture that preserved end-to-end encryption within each platform's domain whilst routing messages through an intermediary layer. BEREC's March 2025 opinion raised concerns about service-level arrangements and access refusal conditions but did not find the architecture incompatible with Article 7 (BEREC, 2025). The paradox is distributional. The architecture suited Meta precisely because it minimised exposure of WhatsApp's core infrastructure to third parties, an outcome the dominant incumbent had the technical resources and negotiating leverage to secure. Signal and Threema, the services most committed to privacy-preserving design, declined to participate on the grounds that the required architecture was incompatible with their own security model. Mandated horizontal interoperability thus produced a configuration in which the dominant incumbent participates under conditions of its own design, whilst the providers operating under more demanding security models are structurally excluded. The result is not a weakest-link dynamic in the classical sense, where the security of an interoperating system degrades to the level of its least secure participant, but its structural inverse: the incumbent's architecture functions as a ceiling that the most security-conscious services cannot meet without compromising their own model, leaving the interoperable ecosystem populated exclusively by services willing to operate on the incumbent's terms.

This is the inverse of the Article 7 objective. The provision was designed to weaken the lock-in effects that sustain WhatsApp's incumbency by enabling users to communicate across platforms without both parties sharing the same service. The implemented architecture achieves a form of interoperability, but at the cost of creating a two-tier ecosystem in which the aggregate security standard available to interoperating users is determined by the least demanding cryptographic model among participating services. As Blessing & Anderson (2023) demonstrate, interoperability in an end-to-end encrypted context creates security interdependencies that operate at the level of the interoperating architecture as a whole, a dynamic that Article 7(9), framed exclusively in terms of the gatekeeper's own security standards and without establishing any benchmark for the interoperability architecture itself, was not designed to address and cannot adequately govern.

3.5. Systemic implications: the trilemma as an interconnected problem

The analysis of the Apple specification proceedings and the WhatsApp interoperability launch yields, across both the vertical and horizontal dimensions, a set of findings that resist reduction to two independent implementation failures. The difficulties identified in each case –regulatory lock-in and the attack surface risk in the vertical dimension; the security paradox and the structural exclusion of privacy-maximising providers in the horizontal dimension– share a common causal origin in the interaction between the DMA's normative architecture and the specific technical characteristics of digital platform ecosystems. Figure 2 maps these findings systematically against the three dimensions of the trilemma, making explicit the causal mechanism that connects the primary-level design defect to the outcomes observed at the implementation stage in each case.

Figure 2.

DMA implementation experience: Apple (vertical) and WhatsApp (horizontal) against the contestability-innovation-security trilemma

Trilemma dimension	Apple iOS specification (Art. 6(7) – vertical) *DMA.100203 and DMA. 100204 implementing acts March 2025*	WhatsApp interoperability (Art. 7 – horizontal) *Launch November 2025*
Contestability	Partially achieved Nine iOS features mandated through prescriptive specification (DMA.100203). Request-based process for further features formalised but subject to comprehensive means-prescription (DMA.100204). Neither channel operates as a genuinely demand-driven model: the first prescribes substance, the second prescribes procedure, leaving limited space for interoperability to be activated proportionately in response to demonstrated third-party need.	Formally achieved; structurally limited Cross-platform messaging enabled for EU users on Meta's terms. Architecture chosen by the dominant incumbent; smaller entrants unable to participate on equivalent terms. Lock-in effect attenuated but not eliminated.
Innovation incentives	Doubly constrained Primary-level parity standard chills investment in new platform features (immediate mandatory access obligation). Secondary level crystallises both specific connectivity features (DMA.100203) and the procedural design of the request-based process (DMA.100204) into binding legal requirements, removing adaptation latitude for both technical and process evolution.	Mixed No direct lock-in of specific technical architecture at secondary level (no Art. 8(2) implementing act). However, BEREC consultation and reference offer review effectively endorse Meta's chosen architecture, creating a de facto standard with first-mover advantage.
Security	Attack surface risk Low-level hardware features (NFC, Bluetooth stack) architecturally designed as closed components. Third-party access creates entry points not accommodated by original iOS security architecture. Apple's derogation claims contested by Commission; independent technical evaluation capacity limited. Whether claims were genuine or strategic cannot be resolved from the public record.	Security paradox Dominant incumbent shaped interoperability architecture to its own infrastructure. Most security-conscious providers (Signal, Threema) excluded by incompatibility with their own security models. Art. 7(9) derogation clause framed around gatekeeper's own standards, not the interoperability architecture as a whole. Result: aggregate security floor set by least demanding participating service.

Causal mechanism	*Primary underdetermination → compliance minimalism → reactive specification proceedings → comprehensive means-prescription of both substance (DMA.100203) and procedure (DMA.100204) → lock-in at secondary level + expanded security contestation space*	*Primary underdetermination → no binding secondary specification → dominant incumbent defines architecture on own terms → security-maximising providers structurally excluded → inverse of Art. 7 objective*

Source: the author based on European Commission (2025), BEREC (2025), Meta (2025) and CEPA (2025).

Figure 2 reveals that the difficulties identified in Sections 3.3 and 3.4 are not three independent regulatory design problems that happen to affect the three vectors of the trilemma separately, nor are they simply two variants of the same problem applied in different technical contexts. They are manifestations of a single systemic failure rooted in the interaction between the DMA's normative architecture –over-inclusive and underdetermined primary-level obligations corrected by a reactive and technically prescriptive secondary level– and the specific characteristics of digital platform ecosystems, in which technical architecture, competitive dynamics and security properties are deeply intertwined. The causal chain runs as follows.

The causal chain runs as follows. The underdetermination of the primary-level obligations shifts the burden of compliance definition to gatekeepers, who, facing broadly framed standards with uncertain boundaries, adopt conservative compliance approaches. The Commission, unable to accept compliance minimalism without undermining the contestability objective, activates specification proceedings[2] to correct it. Those corrective mechanisms, operating under time pressure and without a primary-level proportionality constraint, produce prescriptive-in-means outputs that resolve the primary-level underdetermination by crystallising specific technical standards or architectural choices. Those crystallised standards create lock-in risks in the vertical dimension, compounding the chilling effect on innovation incentives already present at the primary level. In the horizontal dimension, the corrective mechanism produces an architecture that satisfies the dominant incumbent whilst excluding the most security-conscious providers, setting a systemic security floor lower than the Article 7(9) derogation clause contemplates. In both dimensions, gatekeepers facing these constraints invoke security justifications (sometimes genuine, sometimes strategic) to resist or delay compliance, exploiting the operational elasticity of the derogation clauses and placing demands on the Commission's technical institutional capacity that its current enforcement infrastructure is not designed to meet.

The systemic character of this problem has a direct normative implication that shapes the analysis of the comparative cases in Section 4. The difficulties of the DMA's interoperability regime cannot be addressed through incremental adjustments within the existing architecture –clearer guidance on the parity

2 In the vertical dimension through Article 8(2) implementing acts, in the horizontal dimension through the reference offer and BEREC consultation process.

standard, faster specification proceedings and more detailed derogation criteria– because the root cause lies in the fundamental design choice to combine over-inclusive primary-level obligations with underdetermined normative content, relying on reactive secondary-level correction to produce the regulatory clarity the primary level lacks. Whether alternative regulatory architectures have found more coherent resolutions of this trilemma –and at what cost to the contestability objective– is the question that drives the comparative analysis that follows.

4. Comparative analysis: alternative regulatory architectures in the UK and Japan

4.1. Rationale and scope of comparison

The theoretical framework developed in Section 2 identifies three dimensions along which interoperability regulation must be assessed –contestability, innovation incentives and security– and proposes that the optimal regulatory architecture combines outcome-based principles at the primary level with a systematic, procedural specification process at the secondary level. Section 3 demonstrates that the DMA fails to achieve this architecture at either level: its primary-level obligations are simultaneously over-inclusive in scope and underdetermined in normative content, a combination that shifts the burden of compliance definition to gatekeepers and forces the secondary level into a reactive, prescriptive-in-means corrective role that it is structurally ill-suited to perform. The result is a regime that reproduces the weaknesses of both prescriptive and principles-based architectures without capturing the advantages of either.

This section examines the regulatory approaches adopted in the UK and Japan, both of which have enacted legislation addressing digital platform interoperability within the same policy window as the DMA. The comparison is analytically motivated rather than merely descriptive. Both jurisdictions have made distinct architectural choices along the two axes that Section 3 identifies as central: the degree of normative determinacy at the primary level and the character of the secondary specification process. Those choices generate observable variation against the contestability-innovation-security trilemma that is directly illuminated by the systemic analysis of Section 3. The UK and Japan are not presented as superior models, but as sources of regulatory variation that illuminate the trade-offs identified in the theoretical framework and that inform the normative proposals developed in Section 5.

4.2. The UK: the DMCC and the tailored conduct requirement model

4.2.1. Regulatory architecture

The Digital Markets, Competition and Consumers Act 2024 (DMCC) entered into force in January 2025 and established a regulatory framework for digital platforms that differs from the DMA in its fundamental architecture (Digital Markets, Competition and Consumers Act 2024, c. 13). Rather than designating gatekeepers and imposing uniform obligations across all designated entities, the DMCC empowers the Competition and Markets Authority (CMA) to designate firms with Strategic Market Status (SMS) in relation to specific digital activities where they hold substantial and entrenched market power and a position of strategic significance. SMS designation is activity-specific rather than entity-level: a firm may hold SMS in one digital activity without being subject to the regime's obligations in respect of other activities. Designations are time-bound, subject to review every five years, and must be preceded by a nine-month investigation that generates a publicly available evidence base.

Once designated, an SMS firm is subject to conduct requirements (CRs) tailored by the CMA to the firm's specific digital activity and competitive position. The DMCC identifies three categories of objective –fair dealing, open choices, and trust and transparency– but does not specify the substantive content of the conduct requirements that may be imposed. The CMA develops conduct requirements through a structured process involving consultation with the designated firm, third-party stakeholders and, prior to formal designation, publication of an indicative roadmap that sets out the CMA's preliminary assessment of which interventions are likely to be prioritised. This roadmap mechanism, introduced by the CMA in 2025 as an administrative innovation within the DMCC framework, provides regulated entities and third parties with advance visibility of the likely direction of regulatory intervention before formal obligations are imposed (Competition and Markets Authority, 2025a).

In relation to interoperability specifically, the DMCC does not establish any primary-level obligation equivalent to Articles 6(7) or 7 of the DMA. Interoperability is instead addressed as a potential conduct requirement to be imposed on SMS firms where the CMA determines that this is proportionate and serves one of the three statutory objectives. The substance, scope and technical content of interoperability obligations are thereby determined at the secondary level, through the conduct requirement process, rather than being fixed at the legislative level.

4.2.2. Implementation experience

The CMA designated Apple and Google as having SMS in relation to their respective mobile platforms in October 2025, following nine-month investigations that included extensive stakeholder engagement and the publication of roadmaps in July 2025 (Competition and Markets Authority, 2025b). In February 2026 the CMA published proposed commitments from Apple addressing app store fairness and iOS interoperability, and from Google addressing app review, ranking, and data use within the Android ecosystem (Competition and Markets Authority, 2026). In relation to interoperability, Apple committed to allowing developers to request interoperable access to features and functionality within its iOS and iPadOS operating systems, with the CMA evaluating those requests fairly and objectively. The commitments were explicitly framed as a first wave, with further measures anticipated. The CMA indicated that failure to implement the commitments effectively would result in the imposition of formal conduct requirements.

Several features of this process are analytically significant for the purposes of the comparison with the DMA. First, the interoperability commitment obtained from Apple in February 2026 is procedural in character: it establishes a process through which developers can request access to iOS functionality, rather than specifying in advance which features must be made accessible. This is structurally distinct from the DMA's approach in both its primary layer, which specifies a parity standard, and its secondary layer, which identifies specific features through implementing acts. Secondly, the commitment was negotiated rather than imposed unilaterally: Apple's involvement in shaping its content distinguishes it from the DMA's specification decisions, which Apple contested through litigation. Third, the CMA's roadmap mechanism provides a form of advance regulatory signalling that the DMA's reactive specification proceedings do not offer, enabling firms and developers to anticipate the likely direction of regulatory intervention before formal obligations are crystallised.

4.2.3. Assessment against the trilemma

Against the contestability dimension, the DMCC's tailored approach offers meaningful advantages in terms of proportionality and firm-specific calibration. The activity-specific designation process ensures that obligations are imposed only where competitive harm has been evidenced, reducing the risk of over-regulation. The five-year review cycle provides a built-in mechanism for reassessing whether obligations remain appropriate as market conditions evolve. These features reduce the risk of the Type I errors identified in Section 2.3 –over-prescriptive obligations that deter procompetitive conduct–. However, the DMCC also carries a contestability risk that the DMA largely avoids: the absence of primary-level obligations means that no interoperability requirements apply until the CMA has completed a designation investigation and developed tailored conduct requirements, a

process that may take several years from the point at which competitive harm first manifests. The DMA's approach of imposing obligations at designation, with specification proceedings to follow, addresses this gap more directly.

Against the innovation dimension, the DMCC's architecture performs more strongly than the DMA's. By leaving the technical content of interoperability obligations to be determined through a collaborative, firm-specific process, the DMCC avoids the regulatory lock-in risk that arises when specific technical standards are embedded in primary legislation or reactive implementing acts. The roadmap mechanism further reduces the chilling effect on investment by providing advance notice of likely obligations, allowing firms to factor regulatory requirements into their product development cycles rather than facing them as retroactive constraints. The procedural character of the Apple interoperability commitment, establishing a process for evaluating developer requests rather than mandating access to specific features, is particularly well-suited to preserving the technological neutrality that the DMA's secondary level compromises through its feature-specific specification decisions.

Against the security dimension, the DMCC's proportionality-based approach provides meaningful flexibility. The CMA is required to assess proportionality in developing conduct requirements, and the collaborative commitment process allows security considerations to be incorporated into the design of interoperability obligations rather than addressed through post-hoc derogation claims. This reduces the scope for security justifications to function as strategic delay mechanisms, whilst preserving genuine flexibility to address security constraints that cannot be anticipated in advance.

4.3. Japan: the MSCA and the equivalence-based model

4.3.1. Regulatory architecture

Japan's Act on Promotion of Competition for Specified Smartphone Software (MSCA), enacted in June 2024 and entering into force in December 2025, is a third regulatory architecture that occupies a distinct position between the DMA and the DMCC (Smartphone Software Comp etition Promotion Act 2024, Act No. 58 of 2024). The JFTC designated Apple and Google as specified software providers in March 2025, making them subject to the Act's obligations from December 2025 (Japan Fair Trade Commission, 2025a).

The MSCA imposes *ex-ante* obligations that are closer in form to the DMA than to the DMCC: they apply at designation without requiring a separate tailoring process, and the primary legislative text specifies the categories of prohibited conduct and required compliance measures. However, the MSCA

departs from the DMA in two architecturally significant respects. First, the MSCA's interoperability obligation establishes a functional equivalence standard rather than a parity standard. Designated providers are not required to provide access to the same technical means they use themselves, but rather to ensure that third parties can achieve a comparable level of functionality. This formulation preserves greater space for the designated provider to determine the technical means of compliance, reducing the prescriptiveness at the primary level relative to the DMA's parity requirement. Secondly, the MSCA does not prescribe which specific features must be made accessible, leaving the scope of the interoperability obligation to be determined through the JFTC's guidelines and enforcement practice.

The JFTC issued extensive guidelines in July 2025 fleshing out the scope and content of the MSCA's obligations through detailed hypothetical scenarios (Japan Fair Trade Commission, 2025b). A significant feature of those guidelines is that, in interpreting the equivalence standard, the JFTC drew expressly on the European Commission's specification decisions on Apple under Article 6(7) DMA. This cross-jurisdictional normative borrowing is analytically revealing: it demonstrates that specifying technical interoperability standards with sufficient precision is sufficiently difficult that even a well-resourced regulator found it necessary to rely on the prior work of another jurisdiction rather than developing its own technical baseline from scratch. Importantly, however, the MSCA's equivalence standard remains distinct from the DMA's parity standard, so the borrowing is interpretive rather than constitutive. The MSCA's reliance on the DMA's secondary-level outputs thus illustrates both the practical value of prior regulatory specification and the limits of that specification as a transferable model across different primary-level standards.

4.3.2. Implementation experience

The MSCA entered into force in December 2025, making its implementation experience necessarily limited at the time of writing. Apple and Google were designated as specified software providers in March 2025 and have been subject to the Act's obligations since December 2025. The JFTC has indicated its intention to maintain close dialogue with both firms following implementation, with the possibility of requiring further modifications where compliance measures are deemed insufficient. No formal enforcement action or commitment procedure had been concluded at the time of writing. The early implementation period has been characterised by developer disappointment in some respects, particularly regarding the economic viability of alternative payment systems, where platform commissions combined with third-party processing costs frequently exceed the cost of using the platforms' native systems, though these concerns relate primarily to payment obligations rather than interoperability. The JFTC's cooperative, dialogue-based approach to post-designation engagement represents a distinctive feature of the Japanese model that will be of analytical significance as implementation matures.

4.3.3. Assessment against the trilemma

Against the contestability dimension, the MSCA's *ex-ante* approach performs comparably to the DMA in terms of immediacy: obligations apply at designation without requiring a tailoring process. The functional equivalence standard at the primary level provides a clear baseline against which compliance can be assessed, and the JFTC's guidelines reduce uncertainty by providing detailed hypothetical scenarios. However, the Act's reliance on the DMA's specification decisions as an interpretive reference introduces a form of path dependence that limits the MSCA's capacity to develop independently from the DMA's technical standards –including any lock-in embedded in those standards–.

Against the innovation dimension, the MSCA's equivalence standard offers an improvement over the DMA's parity standard at the primary level: by requiring functional equivalence rather than identical access, it preserves greater discretion for designated providers to determine the technical means of compliance, reducing the prescriptiveness-in-means at the primary level. The commitment procedure further supports innovation incentives by allowing designated providers to shape the technical content of their compliance obligations through negotiation with the JFTC. However, the MSCA does not address the reactive character of the secondary specification process: the JFTC's guidelines, whilst detailed, were issued at a single point in time and are not systematically linked to technological cycles.

Against the security dimension, the MSCA's broad justifiable reasons standard provides the most flexible security framework of the three regimes examined. Whether this flexibility translates into effective security protection or merely provides a wider avenue for strategic delay depends on the JFTC's enforcement practice, which remains at an early stage.

4.4. Comparative synthesis

The analysis of the three enacted regimes yields findings that are best organised around the two analytical axes established in Section 3: the degree of normative determinacy at the primary level, and the character of the secondary specification process. Figure 3 maps the three regimes against these axes and against the contestability-innovation-security trilemma.

Figure 3.

Regulatory architecture and trilemma performance: DMA, DMCC, and MSCA compared

Dimension	DMA (EU)	DMCC (UK)	MSCA (Japan)
Regulatory architecture			
Primary level: normative determinacy	Underdetermined Parity standard; over-inclusive and normatively underdetermined; burden of compliance definition falls on gatekeeper	Delegated No primary-level interoperability obligation; entirely delegated to secondary CR process	More determinate Functional equivalence standard; technologically neutral as to means; greater determinacy than DMA parity standard
Primary level: proportionality	Absent at design stage Enters only as parameter of judicial review *ex-post*	Embedded upstream Embedded in designation process and CR development; proportionality assessed upstream	Broad standard Broad justifiable reasons standard; proportionality-like assessment built into compliance evaluation
Secondary level: character	Reactive; prescriptive-in-means Reactive implementing acts (Art. 8(2)); unilateral Commission decision; feature-specific; not linked to technological cycles	Collaborative; prospective Tailored CRs through collaborative, firm-specific process; roadmap provides advance signalling; five-year SMS review	Partially collaborative JFTC guidelines issued at single point in time; commitment procedures introduce collaborative element; not systematically linked to technological cycles
Trilemma performance			
Contestability	Strong but contested Immediate obligations at designation; enforcement signal credible; but parity standard creates compliance minimalism incentive	Delayed Obligations require designation plus CR development, which may take several years	Comparable to DMA Comparable to DMA in immediacy; equivalence standard provides clearer compliance baseline than parity

Innovation incentives	Doubly constrained Parity standard chills new features at primary level; feature-specific implementing acts create lock-in at secondary level	Strong No primary-level lock-in; procedural secondary level preserves technological neutrality; roadmap reduces investment uncertainty	Improved over DMA Equivalence standard reduces primary-level prescriptiveness relative to DMA; commitment procedures partially address secondary-level lock-in; guidelines not systematically updated
Security	Problematic at both levels Attack surface expansion in vertical dimension; weakest-link paradox in horizontal dimension; derogation clauses provide contestable space for strategic delay	Strong Proportionality assessment embedded in CR development; collaborative process allows proactive security incorporation; reduces scope for strategic invocation of security	Flexible; untested Broad justifiable reasons standard provides most flexible framework; effectiveness depends on JFTC enforcement capacity, which remains untested
Additional dimensions			
Technological neutrality	Compromised at secondary level Primary level formally neutral; secondary level compromised by feature-specific implementing acts	Preserved at both levels Preserved at both levels through procedural secondary process	Partially compromised Primary level neutral; secondary level partially compromised by DMA-referencing guidelines
Systematic review	None Reactive proceedings only; structurally in catch-up mode	Partial Five-year SMS designation review; roadmap updated periodically	None Guidelines issued once; no systematic review mechanism

Source: the author.

Figure 3 reveals a pattern that is analytically significant beyond the individual assessments of each regime. No enacted regime achieves full coherence across both axes simultaneously. The DMA performs most strongly on contestability –its immediate, uniform obligations at designation provide a credible enforcement signal that neither the DMCC nor the MSCA fully replicates– but it does so at the cost of a double structural defect: normative underdetermination at the primary level that incentivises compliance minimalism, and reactive prescription at the secondary level that creates lock-in and a permanent catch-up deficit. The DMCC inverts this trade-off: by delegating entirely to a collaborative, firm-specific secondary process, it achieves the strongest performance on innovation and security, preserving

technological neutrality at both levels and embedding proportionality upstream, but it sacrifices the immediacy of contestability protection that the DMA's primary-level obligations provide. The MSCA occupies an intermediate position on both axes: its functional equivalence standard is more normatively determinate than the DMA's parity standard whilst preserving greater compliance discretion than a means-specific obligation, and its commitment procedures introduce a collaborative element at the secondary level that the DMA lacks, but its guidelines were issued at a single point in time and are not systematically linked to technological cycles.

4.5. Emerging jurisdictions and the diffusion of regulatory models

The comparative analysis of the EU, UK and Japan reveals that the choice of regulatory architecture for digital platform interoperability has material consequences for the contestability-innovation-security trilemma. This finding has relevance beyond the three jurisdictions examined, as a growing number of countries are in the process of designing or legislating *ex-ante* digital competition regimes. The experience of these emerging jurisdictions is analytically significant for two reasons: it illustrates the extent to which existing regulatory models are being consciously adopted, adapted or rejected as templates; and it identifies the architectural choices that jurisdictions with the advantage of hindsight are making in light of the implementation experience of the DMA, the DMCC and the MSCA.

Australia provides the most developed example of a jurisdiction explicitly self-positioning as a fast follower. Following eight years of sequential ACCC inquiries into digital platform services (Australian Competition and Consumer Commission, 2025), the Australian Government announced its intention in December 2023 to introduce an *ex-ante* digital competition regime, with Treasury consulting on a proposed framework through February 2025. The ACCC's final Digital Platform Services Inquiry report, published in June 2025, endorsed the case for *ex-ante* regulation and explicitly reviewed the DMA, the DMCC and the MSCA as comparative reference points, noting that overseas jurisdictions had acknowledged the inadequacy of existing competition tools in the face of the digital markets' rapidly evolving nature. The proposed Australian framework departs from the DMA model in a manner that is architecturally significant for the purposes of this analysis: rather than establishing uniform primary-level obligations applicable to all designated platforms, it envisages service-specific codes of conduct developed through a collaborative process between the ACCC and designated platforms, with interoperability obligations addressed as targeted, service-specific requirements rather than as universally applicable primary-level rules (Australian Competition and Consumer Commission, 2025). This architecture

is closer to the DMCC model than to the DMA, preserving flexibility at the secondary level whilst maintaining a clear primary-level framework for designation and enforcement. Legislation had not been enacted at the time of writing.

Canada presents a contrasting case of a jurisdiction that has pursued significant reforms to its competition law framework –through Bills C-19, C-56, and C-59, amending the Competition Act– without yet enacting a dedicated *ex-ante* regime for digital platforms (Competition Bureau Canada, 2025). Interoperability features in Canadian policy discourse as a desiderata, appearing in the government's Digital Charter principles and in consultations on open banking and data mobility, but has not been translated into primary-level legislative obligations for digital gatekeepers. Canada's trajectory illustrates the path-dependence of competition law systems: the incremental reinforcement of ex-post enforcement tools, rather than the adoption of a distinct *ex-ante* architecture, reflects an institutional preference for working within existing frameworks rather than establishing a separate regulatory regime.

India and South Korea represent two further points of reference. India's Committee on Digital Competition Law published a detailed report in February 2024 proposing an *ex-ante* framework closely modelled on the DMA, including interoperability obligations for significant digital enterprises (Ministry of Corporate Affairs, India, 2024). The proposal has not yet been enacted and remains under legislative consideration. South Korea's Korea Fair Trade Commission proposed DMA-style platform regulation in December 2023, similarly focused on self-preferencing, interoperability and data access (Korea Fair Trade Commission, 2023). Both proposals illustrate the DMA's role as a primary template for jurisdictions designing *ex-ante* regimes from scratch, a form of regulatory diffusion that carries with it not only the DMA's strengths but also the architectural weaknesses identified in Section 3, including the reactive character of the secondary specification process and the lock-in risk at the level of implementing measures.

The pattern that emerges from this broader landscape is analytically significant. Jurisdictions that have enacted legislation –the EU, the UK and Japan– have made distinct architectural choices that reflect different resolutions of the contestability-innovation-security trilemma. Jurisdictions still in the design phase –Australia, India and South Korea– face a genuine choice between replicating the DMA's architecture wholesale, adapting it in the direction of the DMCC's procedural secondary level, or developing hybrid models. The normative argument developed in Section 5 is therefore directly relevant not only to the revision of the DMA but to the design choices facing this wider group of jurisdictions. The advantage of the fast follower is precisely that it can internalise the implementation lessons of the first movers before they are locked into a regulatory architecture that is difficult to reform.

5. Towards a coherent regulatory architecture: normative proposals and conclusions

5.1. The normative task

The analysis developed in the preceding sections generates a diagnostic conclusion that is precise enough to be actionable. The DMA's interoperability regime fails not because it is too prescriptive or too permissive, but because it is incoherent across normative levels: its primary-level obligations are over-inclusive and normatively underdetermined, generating a secondary level that is reactive and prescriptive-in-means, a combination that produces the weaknesses of both prescriptive and principles-based architectures without capturing the advantages of either. The comparative analysis of Section 4 demonstrates that this incoherence is not inevitable: the DMCC and, to a lesser extent, the MSCA have made distinct architectural choices that generate more balanced outcomes across the contestability-innovation-security trilemma, at varying costs to the immediacy of contestability protection. And the diffusion analysis of Section 4.5 shows that the architectural choices made now will shape the design of regimes across a growing number of jurisdictions for which the DMA functions as a primary template.

The normative proposals that follow address the three structural deficits identified by the analysis: the normative underdetermination of the primary level, the reactive and prescriptive character of the secondary level, and the institutional incapacity that prevents either level from functioning as intended. These are not independent proposals but three interlocking dimensions of a single architectural reform. The first two can be pursued as amendments within the current DMA review cycle; the third requires a more fundamental institutional commitment whose implications extend beyond interoperability to the full architecture of EU digital regulation.

5.2. First proposal: normative determinacy at the primary level

The root cause of the DMA's interoperability failures is not the absence of technical specification at the primary level –a coherent principles-based regime does not require it– but the absence of sufficient normative determinacy to orient compliance, constrain specification discretion at the secondary level and provide a basis against which the adequacy of any proposed implementation can be assessed. The parity standard of Article 6(7) and the basic functionality standard of Article 7 fail this test not because they avoid technical means –this is appropriate– but because they do not articulate the outcome criteria by which any proposed technical means is to be evaluated.

The reform required at the primary level is therefore not a shift towards prescriptiveness but a shift towards what might be termed outcome-determinacy: the articulation, in the primary legislative text, of the functional results that compliant interoperability must achieve, the criteria by which those results are to be assessed, and the proportionality boundaries within which the secondary level may specify implementation. This is the approach that the EU telecoms regime has long employed, requiring national regulatory authorities to select the least intrusive obligation capable of addressing the identified market failure, and it is the approach that distinguishes the DMCC's conduct requirements, which are calibrated to identified competitive harm, from the DMA's uniform primary-level obligations.

Specifically, for the vertical dimension, Article 6(7) should be reformulated to specify that third parties must be able to achieve a level of functional access that does not place them at a material competitive disadvantage relative to the gatekeeper's own vertically integrated services, evaluated by reference to criteria including the timeliness of access, the technical completeness of the interface, and the absence of conditions that are not objectively justified by security or integrity concerns. These outcome criteria serve a dual function. At the level of the gatekeeper, they define the standard against which the request-based process must deliver. At the level of the regulatory authority, they provide the benchmark for assessing whether the process is functioning effectively. The shift from means-prescription to outcome-determinacy thus applies not only to the substance of the interoperability obligation but to the trigger for regulatory intervention.

For the horizontal dimension, the reform is more complex because Article 7's underdetermination is compounded by the specific technical characteristics of end-to-end encrypted messaging, which mean that the security implications of any proposed architecture cannot be evaluated by reference to a simple outcome criterion. The appropriate reform here is not simply a restatement

of the outcome but an explicit requirement that the Commission develop, through a structured and technically expert process, a set of minimum security benchmarks for interoperable messaging architectures. This converts the security derogation from a space of strategic ambiguity into a boundary defined by technical criteria, whilst preserving the flexibility for gatekeepers to determine the means of achieving interoperability that satisfies those criteria.

Both reforms share a common logic: they do not reduce the ambition of the primary-level obligations but make that ambition governable, by specifying the results to be achieved and the criteria by which achievement is to be assessed, whilst leaving the technical means to be determined at the secondary level. This is the architecture that the central argument of this paper has consistently described as optimal, and it is the architecture that the DMA's primary level currently fails to provide.

5.3. Second proposal: a demand-driven secondary level with proportionate regulatory oversight

The second structural deficit is the reactive, unilateral and feature-specific character of the Article 8(2) specification mechanism. As the analysis of Section 3.3 demonstrates, this mechanism functions not as a systematic process for translating outcome-based principles into technical standards but as a corrective for the underdetermination of the primary level. The additional analysis of DMA.100204 reveals that the problem extends beyond the substance of specification to the procedure: the Commission has prescribed not only which features must be opened but also the detailed means by which the gatekeeper must administer its own request-based process. The reform required here is architectural: the specification mechanism must be redesigned to treat the gatekeeper's request-based process as the primary channel for delivering interoperability, with specification proceedings reserved as a residual mechanism activated by evidence that the process is failing to meet defined outcome criteria.

The CMA's roadmap mechanism, introduced as an administrative innovation within the DMCC framework in 2025, provides a partial model. By publishing in advance the likely direction of regulatory intervention before formal obligations are imposed, the roadmap reduces investment uncertainty, enables regulated entities to factor regulatory requirements into product development cycles and generates a structured basis for stakeholder input before specifications are crystallised (Competition and Markets Authority,

2025a). The DMA's current Article 8(2) mechanism provides no equivalent: specification proceedings are opened in response to identified compliance failures and produce unilateral implementing acts that regulated entities can contest only through litigation. However, the CMA model also illustrates the limits of proactive regulatory signalling: even advance notice of likely intervention presupposes that the regulator, rather than market demand, determines which features warrant interoperability. The demand-driven model proposed here goes further: the gatekeeper's process, operating against defined outcome criteria, determines the pace and scope of interoperability, with the regulatory authority monitoring the process's effectiveness rather than directing its content.

The proposed reform has two elements. First, the principal mechanism for activating interoperability in the vertical dimension should be a gatekeeper-administered request-based process through which third parties can seek access to specific features. The *ex-ante* obligation should define the outcome criteria that this process must satisfy, without prescribing the detailed procedural means by which the gatekeeper administers the process. The regulatory authority's role should be to assess whether the process delivers effective interoperability against those outcome criteria, and to intervene proportionately where it does not. This architecture would treat the request-based process as the primary channel and prescriptive specification as a residual instrument, inverting the current hierarchy in which prescriptive specification operates as the default and the request-based process is itself subject to comprehensive means-prescription.

Secondly, where the regulatory authority determines that the gatekeeper's request-based process is failing to deliver against the defined outcome criteria and specification proceedings are warranted, the specification process itself should be collaborative rather than unilateral. This does not mean that the outcome of the process should be negotiated, but that the technical content of specifications should be developed through a structured multi-stakeholder process involving designated gatekeepers, third-party requesters and technical expert bodies, with transparent documentation of the choices made and their justifications. The collaborative process should be informed by evidence of actual market conditions, including data on the volume and nature of interoperability requests, third-party adoption rates of existing interoperability solutions, and documented instances where the gatekeeper's request-based process has failed to deliver against the outcome criteria defined at the primary level, ensuring that specification effort is directed towards areas of demonstrated need rather than allocated on the basis of the regulator's *ex-ante* assessment of which features ought to be interoperable.

Together, these two elements –a demand-driven request-based process as the primary channel and collaborative specification as the residual mechanism– would transform the secondary level from a regime of comprehensive means-prescription into one that combines *ex-ante* outcome obligations with

proportionate regulatory intervention, reserving the most intrusive instruments for cases where the gatekeeper's own process demonstrably fails to deliver effective interoperability.

5.4. Third proposal: an independent European digital authority

The third structural deficit is the most fundamental and the most consequential beyond the specific context of interoperability regulation. The analysis of Sections 3.3 and 3.4 demonstrates that the security problems identified in both the vertical and horizontal dimensions of the DMA's interoperability regime are not primarily problems of normative design, but problems of institutional architecture. The institutional challenge has two analytically distinct dimensions that are often conflated in the literature but should be kept separate. The first is a question of capacity: the Commission lacks the technical expertise and institutional continuity necessary to evaluate compliance with technically complex obligations with sufficient authority and speed to prevent claims of security or integrity from becoming instruments of strategic delay. The second is a question of impartiality: the Commission simultaneously defines primary-level obligations, opens specification proceedings, conducts the technical evaluation, adopts the implementing act, defends the act in litigation and manages the political consequences of the outcome, a configuration in which the institution evaluating gatekeeper compliance is not structurally disinterested in the evaluation's result. Capacity constraints admit incremental solutions –more technical staff, longer timelines, enhanced consultation procedures– but impartiality constraints are architectural: they can be addressed only through institutional separation between the functions of rule-setting, adjudication and enforcement. The case for an independent European digital authority rests on both dimensions, but it is the impartiality dimension that renders incremental reform within the existing architecture structurally insufficient.

This institutional deficit is not specific to interoperability. The Commission's enforcement of the DMA, DSA and AI Act simultaneously as political body, regulatory authority, specification agency and enforcement organ places demands on a single institution that are structurally incompatible with the credibility and technical depth that effective digital regulation requires. The evidence is accumulating across multiple dimensions: the Commission's DMA enforcement unit has faced persistent staffing constraints acknowledged by its own senior officials; the pace of specification proceedings is structurally misaligned with the pace of technological change; and the Commission's exposure to geopolitical pressure –documented in the context of DSA

enforcement and increasingly visible in the DMA context through US-EU trade negotiations– creates a structural risk that regulatory outcomes will be influenced by considerations extraneous to the regulatory objectives (Mariniello, 2026; Harfst, Mast & Schulz, 2025; Centre for Future Generations, 2025).

The case for an independent European digital authority is not new, but the implementation experience of the past three years has sharpened its urgency and clarified its content. Mariniello (2026) has made the most recent and analytically rigorous case, arguing that an independent agency modelled on ESMA or AMLA –with direct enforcement powers, fee-based funding independent of the Commission's budgetary process, and governance structures insulated from political interference through fixed-term appointments and CJEU accountability– would reduce the risk of both over-enforcement driven by regulatory zeal and under-enforcement driven by geopolitical pressure, whilst developing the institutional memory and technical expertise that effective digital regulation requires over time. Harfst, Mast & Schulz (2025) reach a similar conclusion specifically for DSA enforcement, noting that the Commission's structural inability to insulate its enforcement decisions from political considerations constitutes a rule-of-law problem, not merely an institutional efficiency problem.

The argument developed in this paper adds a dimension to this literature that has not been sufficiently emphasised in previous contributions: an independent digital authority is not only desirable for the enforcement of existing obligations but is a precondition for the functioning of the two proposals advanced in Sections 5.2 and 5.3. The outcome-determinate primary level proposed in Section 5.2 requires an authority capable of translating functional criteria into technical assessments of compliance, a capability that requires sustained technical expertise and institutional continuity that the Commission's current enforcement architecture does not possess. The demand-driven secondary level proposed in Section 5.3 requires an authority capable of defining and monitoring outcome criteria across multiple gatekeeper ecosystems, evaluating evidence of process failure when third parties or market indicators signal it, and managing collaborative specification processes in the residual cases where prescriptive intervention is warranted.

The scope of the proposed authority warrants careful consideration. Mariniello (2026) argues, plausibly, that the case for independence is currently stronger for DSA enforcement than for DMA enforcement, given the DMA's closer integration with competition law and the Commission's accumulated expertise in that field. The analysis of this paper suggests, however, that the interoperability provisions of the DMA, and specifically the specification function under Article 8(2), represent a distinct category within DMA enforcement that is better characterised as technical regulation than as competition enforcement, and that this distinction justifies delegating the specification function to a body with the technical mandate and institutional independence appropriate to that role, even if broader DMA enforcement

remains with the Commission. The ESMA model is instructive here: ESMA's direct supervisory authority over credit rating agencies and critical market infrastructure was introduced as a targeted extension of its mandate into areas requiring technical expertise and operational independence, without requiring the wholesale transfer of EU competition policy to an external agency.

The proposed authority would therefore have, at minimum, four functions relevant to the interoperability context. First, the definition and monitoring of outcome criteria against which gatekeepers' request-based processes are assessed. Secondly, the management of collaborative specification processes in the residual cases where the request-based process demonstrably fails, including the evaluation of integrity and security claims made by gatekeepers under the derogation clauses of Articles 6(7) and 7(9) respectively, with access to the independent technical expertise necessary to distinguish genuine constraints from strategic invocations. Third, the assessment of whether specification outputs remain adequate as technology evolves, with the capacity to recommend targeted amendments where warranted by evidence rather than conducting comprehensive periodic reviews. Fourth, the enforcement of outcome criteria and, where applicable, specification decisions against gatekeepers, with powers equivalent to those currently exercised by the Commission under Article 8(2) but insulated from the geopolitical pressures that the Commission's broader institutional position makes it structurally difficult to resist.

The constitutional constraints on this proposal are real but not prohibitive. The Meroni doctrine, as interpreted by the CJEU, permits the delegation of clearly defined technical tasks to independent agencies without treaty amendment, provided the discretion delegated is bounded by the terms of the primary legislative act and subject to judicial review. The specification function under Articles 6(7) and 8(2) is precisely the kind of technically bounded, judicially reviewable function that falls within the Meroni framework: it does not require the open-ended political discretion that the doctrine prohibits but the sustained technical expertise and institutional continuity that independent agencies are specifically designed to provide. The Commission could retain designation authority, whilst delegating the outcome monitoring, residual specification and enforcement to an independent body. This division of functions replicates, in the digital context, the architecture that has proved effective in EU financial regulation, where the Commission retains legislative initiative whilst ESMA and AMLA exercise direct supervisory and enforcement authority over the most technically demanding aspects of financial market regulation.

Conclusions

The DMA's interoperability regime was designed to restore contestability to digital platform markets by compelling gatekeepers to open the infrastructure on which competitive entry depends. That objective remains as urgent as when the Regulation was conceived. What the implementation experience of the past three years demonstrates is that the pursuit of contestability through a normatively underdetermined primary level and a reactive, prescriptive secondary level does not achieve that objective. It displaces the problem, generating compliance minimalism, regulatory lock-in and security paradoxes that the existing architecture is structurally ill-equipped to resolve. The proposals advanced in this paper are not a retreat from the ambition of *ex-ante* intervention but the institutional preconditions for making that ambition governable.

The three proposals are analytically interlocking and their combined effect on the trilemma can be stated precisely. For contestability, outcome-determinacy at the primary level (Section 5.2) provides third parties with clear criteria against which to assess the gatekeeper's compliance, eliminating the normative ambiguity that currently incentivises compliance minimalism; the demand-driven secondary level (Section 5.3) ensures that interoperability is activated where there is demonstrated need, directing regulatory attention toward concrete competitive harm rather than dispersing it across a comprehensive but unfocused mapping of technically feasible access points; and the independent authority (Section 5.4) provides the institutional capacity to monitor the process's effectiveness and to intervene credibly where it fails. For innovation, outcome-determinacy eliminates the chilling effect of a parity standard that subjects every new feature to immediate mandatory access, replacing it with a functional criterion that preserves the gatekeeper's latitude to determine the technical means of compliance; the demand-driven secondary level avoids the crystallisation risk of prescriptive implementing acts by allowing the gatekeeper to design tailored solutions in response to specific requests, consistent with its own development cycle; and the independent authority's monitoring function, calibrated to outcome criteria rather than comprehensive means-prescription, reduces the

regulatory burden that currently scales with the number of features, platforms and gatekeepers subject to the regime. For security, outcome-determinacy establishes the benchmarks against which security claims are assessed, converting the derogation clause from a space of strategic ambiguity into a boundary defined by technical criteria; the demand-driven secondary level allows security implications to be evaluated case by case at the point of request, rather than contested wholesale after a binding implementing act has been adopted; and the independent authority provides the sustained technical expertise necessary to distinguish genuine security constraints from strategic invocations –a function that the Commission's current enforcement infrastructure, as the implementation experience of Sections 3.3 and 3.4 demonstrates, does not consistently possess–.

The DMA review cycle, and the wider community of jurisdictions now drawing on its architecture as a template, offers a precise and time-limited opportunity to internalise these lessons before they are encoded into a second generation of regulatory frameworks as difficult to reform as the first.

References

Aghion, P., N. Bloom, R. Blundell, R. Griffith & P. Howitt (2005), 'Competition and innovation: an inverted-U relationship', *Quarterly Journal of Economics*, vol. 120, nr 2, p. 701-728, https://doi.org/10.1162/0033553053970214.

Armstrong, M. (2006), 'Competition in two-sided markets', *RAND Journal of Economics*, vol. 37, nr 3, p. 668-691, https://doi.org/10.1111/j.1756-2171.2006.tb00037.x.

Arrow, K.J. (1962), 'Economic welfare and the allocation of resources for invention', in R.R. Nelson (Ed.), *The Rate and Direction of Inventive Activity: Economic and Social Factors*, Princeton University Press, p. 609-626.

Australian Competition and Consumer Commission (2025), *Digital Platform Services Inquiry: Final Report*, ACCC, 23/VI/2025, https://www.accc.gov.au/inquiries-and-consultations/finalised-inquiries/digital-platform-services-inquiry-2020-25/march-2025-final-report.

Baldwin, R., M. Cave & M. Lodge (2012), *Understanding Regulation: Theory, Strategy, and Practice*, 2nd edition, Oxford University Press.

Black, J. (2008), 'Forms and paradoxes of principles-based regulation', *Capital Markets Law Journal*, vol. 3, nr 4, p. 425-457, https://doi.org/10.1093/cmlj/kmn026.

Blessing, J., & R. Anderson (2023), 'One protocol to rule them all? On securing interoperable messaging', in F. Stajano, V. Matyáš, B. Christianson & J. Anderson (Eds.), *Security Protocols XXVIII*, Lecture Notes in Computer Science, vol. 14186, Springer, p. 184-200, https://doi.org/10.1007/978-3-031-43033-6_17.

Body of European Regulators for Electronic Communications (2025), 'BEREC opinion on Meta's reference offers to facilitate Messenger and WhatsApp interoperability under Article 7 of the Digital Markets Act (BoR (25) 21)', BEREC, 3/III/2025, https://www.berec.europa.eu/en/all-documents/berec/opinions/berec-opinion-on-metas-reference-offers.

British Government (2024), 'Digital Markets, Competition and Consumers Act 2024 (c. 13)', https://www.legislation.gov.uk/ukpga/2024/13.

Centre for European Policy Analysis (2025), *Opening Up – Europe's DMA and the Risks of Interoperability*, CEPA, 3/XII/2025, https://cepa.org/article/part-2-opening-up-europes-dma-and-the-risks-of-interoperability/.

Centre for Future Generations (2025), 'Enforcement spotlight – Autumn 2025', January, https://cfg.eu/enforcement-spotlight-autumn-2025/.

Competition and Markets Authority. (2025a), 'SMS investigation into Apple's mobile platform: indicative roadmap', CMA, 23/VII/2025, https://www.gov.uk/cma-cases/sms-investigation-into-apples-mobile-platform.

Competition and Markets Authority. (2025b), 'CMA confirms Apple and Google have strategic market status in mobile platforms', CMA, press release, 22/X/2025, https://www.gov.uk/government/news/cma-confirms-apple-and-google-have-strategic-market-status-in-mobile-platforms.

Competition and Markets Authority (2026), 'CMA secures commitments from Apple and Google to improve fairness in app store processes and enhance iOS interoperability', CMA, press release, 10/II/2026, https://www.gov.uk/government/news/cma-secures-commitments-from-apple-and-google-to-improve-fairness-in-app-store-processes-and-enhance-ios-interoperability.

Competition Bureau Canada (2025), *Competition Act amendments: Bills C-19, C-56, and C-59 – Overview of reforms*, Government of Canada, https://www.competitionbureau.gc.ca.

Crémer, J., Y.-A. de Montjoye & H. Schweitzer (2019), 'Competition policy for the digital era', European Commission, https://op.europa.eu/en/publication-detail/-/publication/21dc175c-7b56-11e9-9f05-01aa75ed71a1.

Easterbrook, F.H. (1984), 'The limits of antitrust', *Texas Law Review*, vol. 63, nr. 1, p. 1-40.

European Commission (2025), 'Digital Omnibus simplification package', Legislative proposal, https://digital-strategy.ec.europa.eu/en/policies/digital-omnibus.

European Commission (2025), '*Summary of Commission Decision of 19 March 2025 –Case DMA.100203–Apple–iOS* (OJ C 2025/4646)', Publications Office of the EU, 19/III/2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202504646.

European Commission (2026), 'Commission opens proceedings to assist Google in complying with interoperability and online search data sharing obligations under the Digital Markets Act', press release, 27/I/2026, https://digital-markets-act.ec.europa.eu/commission-opensproceedings-assist-google-complying-interoperability-and-online-search-data-sharing-2026-01-27_en.

European Union (2022), 'Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), OJ L 265', 12/X/2022, p. 1-66.

Farrell, J., & G. Saloner (1985), 'Standardization, compatibility, and innovation', *RAND Journal of Economics*, vol. 16, nr 1, p. 70-83, https://doi.org/10.2307/2555589.

Geradin, D., & D. Katsifis (2022), 'Selecting the right regulatory design for pro-competitive digital regulation: an analysis of the EU, UK, and US approaches', SSRN Working Paper, https://doi.org/10.2139/ssrn.4025419.

Harfst, J.-O., T. Mast & W. Schulz (2025), 'Independence as a desideratum: DSA enforcement by the EU Commission', *Verfassungsblog*.16/VII/2025, https://verfassungsblog.de/dsa-enforcement-commission/.

Ibáñez Colomo, P. (2021), 'The draft Digital Markets Act: a legal and institutional analysis', *Journal of European Competition Law & Practice*, vol. 12, nr 7, p. 561-575, https://doi.org/10.1093/jeclap/lpab065.

Information Technology and Innovation Foundation (2022), 'The Digital Markets Act: a triumph of regulation over innovation, ITIF, 24/VIII/2022, https://itif.org/publications/2022/08/24/digital-markets-act-a-triumph-of-regulation-over-innovation/.

Jacobides, M.G., C. Cennamo & A. Gawer (2018), 'Towards a theory of ecosystems', *Strategic Management Journal*, vol. 39, nr 8, p. 2255-2276, https://doi.org/10.1002/smj.2904.

Japan Fair Trade Commission (2024), 'Smartphone Software Competition Promotion Act 2024 (Act on Promotion of Competition for Specified Smartphone Software), Act No. 58 of 2024', JFTC, 12/VI/2024, https://www.jftc.go.jp/en/policy_enforcement/digital/index.html.

Japan Fair Trade Commission (2025a), 'Designation of specified software operators under the Act on Promotion of Competition for Specified Smartphone Software', JFTC, 31/III/2025, https://www.jftc.go.jp/en/pressreleases/yearly-2025/March/250331.html.

Japan Fair Trade Commission (2025b), 'Mobile Software Competition Act guidelines', JFTC, 29/VII/2025, https://www.jftc.go.jp/en/pressreleases/yearly-2025/July/250729.html.

Katz, M.L., & C. Shapiro (1985), 'Network externalities, competition, and compatibility', *American Economic Review*, vol. 75, nr 3, p. 424-440.

Kerber, W., & H. Schweitzer (2017), 'Interoperability in the digital economy', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 8, nr 1, p. 39-58, https://www.jipitec.eu/issues/jipitec-8-1-2017/4531.

Korea Fair Trade Commission (2023), 'Proposal for ex ante platform regulation: Self-preferencing, interoperability, and data access', December, https://www.ftc.go.kr/en.

Larouche, P., & A. de Streel (2021), 'The European Digital Markets Act: a revolution grounded on traditions', *Journal of European Competition Law & Practice*, vol. 12, nr 7, p. 542-560, https://doi.org/10.1093/jeclap/lpab066.

Lemley, M.A., & D. McGowan (1998), 'Legal implications of network economic effects', *California Law Review*, vol. 86, nr 3, p. 479-611, https://doi.org/10.2307/3481186.

Lundqvist, B. (2024), 'Europe's DMA: answering ambiguity', Centre for European Policy Analysis, 29/III/2024, https://cepa.org/article/europes-dma-answering-ambiguity/.

Manne, G.A., & J.D. Wright (2010), 'Innovation and the limits of antitrust', *Journal of Competition Law & Economics*, vol. 6, nr 1, p. 153-202, https://doi.org/10.1093/joclec/nhp036.

Mariniello, M. (2026), 'The case for a European Union digital enforcement authority', *Policy Brief*, nr 05/2026, February, Bruegel, https://doi.org/10.64153/JLNI2855.

Meta (2025), 'Messaging interoperability: WhatsApp enables third-party chats for users in Europe', blog post, 14/XI/2025, https://about.fb.com/news/2025/11/messaging-interoperability-whatsapp-enables-third-party-chats-for-users-in-europe/.

Ministry of Corporate Affairs (2024), *Report of the Committee on Digital Competition Law*, Government of India, February, https://www.mca.gov.in.

Ribera Martínez, A. (2025), 'Interoperability by design or denial? The Digital Markets Act's notion of vertical interoperability', SSRN Working Paper, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5121387.

Rochet, J.-C., & J. Tirole (2003), 'Platform competition in two-sided markets', *Journal of the European Economic Association*, vol. 1, nr 4, p. 990-1029, https://doi.org/10.1162/154247603322493212.

Schumpeter, J.A. (1942), *Capitalism, Socialism and Democracy*, Harper & Brothers.

Author

Judith Arnal, Senior Fellow and member of the Scientific Council, Elcano Royal Institute

Recommended citation:

Arnal, Judith (2026), "Contestability, innovation, security: resolving the trilemma of digital platform interoperability regulation", *Elcano Policy Paper*, Elcano Royal Institute

Board of Trustees

GOBIERNO DE ESPAÑA — MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN

GOBIERNO DE ESPAÑA — MINISTERIO DE DEFENSA

GOBIERNO DE ESPAÑA — MINISTERIO DE CULTURA

GOBIERNO DE ESPAÑA — MINISTERIO DE ECONOMÍA, COMERCIO Y EMPRESA

ACERINOX · ACS · AIRBUS · amazon · BBVA · BANCO DE ESPAÑA Eurosistema · CaixaBank · Cámara de Comercio de España · em&e group · enagas · endesa · GARRIGUES · Hijos de Rivera · Iberdrola · IBM · INDITEX · INDRA GROUP · INSUD PHARMA · MADRID · moeve · MUTUAMADRILEÑA · Naturgy · oesia · PROSEGUR · renfe · repsol · Santander · Telefónica

Protector Partners

acciona · CAF Banco de Desarrollo de América Latina y el Caribe · El Corte Inglés · Google · Sabadell

Collaborating Partners

//ABANCA · aena · aws · ceca · cesce Seguros de tu éxito · Deloitte. · Fundación Ibercaja · KPMG · mapfre · NETFLIX

Real Instituto Elcano
Príncipe de Vergara, 51
28006 Madrid (Spain)
www.realinstitutoelcano.org