International Journal of Innovative Inventions in Social Science and Humanities

ISSN(print): 3050-6921, ISSN(online): 3050-693X

Volume 03 Issue 11 November 2026

DOI: 10.58806/ijiissh.2026.v3i11n13

Page No: 1660-1677

Cybersecurity as a Market Power Problem: Competition Law, Interoperability and the Economics of Digital Dependence

Dr Godwin Gaduga

Lecturer at Accra Institute of Technology Adjunct Lecturer at Blue Crest University College

ABSTRACT

Dominant digital firms increasingly defend closed systems in the language of security, and that language carries unusual weight because it invokes harms that regulators fear, that courts find difficult to evaluate and that consumers cannot observe. This article contends that cybersecurity is not merely a technical attribute of digital products but a variable of market power, since the firm that controls the interfaces through which security is defined, certified and enforced also controls who may compete on and around its platform. Reading the Electronic Communications Act 2008 (Act 775), the Payment Systems and Services Act 2019 (Act 987), the Cybersecurity Act 2020 (Act 1038), the Evidence Act 1975 (NRCD 323) and the 1992 Constitution alongside the interoperability jurisprudence of the European Union, the United States, the United Kingdom and South Africa, the article proposes the Security Necessity and Symmetry Test, a seven-stage inquiry for distinguishing genuine security restrictions from competitive restraints that are justified in security terms. The test has three distinctive features: a symmetry principle, under which a dominant firm that exempts its own services from a restriction it imposes on rivals bears a rebuttable presumption of pretext; a requirement that the security rationale have existed when the restriction was adopted; and an allocation of evidential burdens that follows informational control rather than the formal posture of the parties. Although Ghana still lacks a general competition statute, the article shows that the test can be applied at once through existing sectoral powers over significant market power and through constitutional administrative law, and it proposes judicial, regulatory and legislative reforms designed to discipline pretext without weakening the protections on which a digital economy depends.

ARTICLE DETAILS

Published On:
16 November 2026

KEYWORDS: Competition Law, Cybersecurity, Interoperability, Abuse Of Dominance, Significant Market Power, Switching Costs, Lock-In, Ghana, Digital Markets Act, Objective Justification.

Available on:
https://ijiissh.com/

I. INTRODUCTION

In 2018, Google declined to make JuicePass, an Italian application for locating and booking electric vehicle charging points, compatible with Android Auto. Among the reasons it gave were security concerns and the absence of a template for that category of application.[1] Apple has resisted the opening of its operating system to rival app distribution, payment services and device connectivity, and in litigation and public debate the argument that has carried most weight is the protection of users against malware, fraud and intrusion.[2] In August 2025 Google announced that every developer distributing Android applications outside its own store would have to register with Google and verify its identity before those applications could be installed on certified devices, with enforcement beginning in Brazil, Indonesia, Singapore and Thailand on 30 September 2026; the stated purpose was, once again, the

[1] Case C-233/23 *Alphabet Inc and Others v Autorità Garante della Concorrenza e del Mercato* (CJEU, 25 February 2025); Court of Justice, press release on the judgment in Case C-233/23 (25 February 2025), recording that Google justified its refusal on security grounds and on the need to allocate the resources required to create a new template.

[2] *Epic Games Inc v Apple Inc* 67 F 4th 946 (9th Cir 2023), cert denied 144 S Ct 682 (2024).

deterrence of malicious actors.[3] None of these justifications was frivolous. Each, however, was advanced by a firm that stood to gain commercially from the restriction it defended, and it is that coincidence of a genuine public interest with a private competitive advantage which this article examines.

That security matters are not in doubt, and a legal framework that treated security claims with reflexive suspicion would expose citizens, financial systems and critical information infrastructure to harms that no competition remedy could repair. The difficulty lies elsewhere. A security justification for a closed system, a restricted interface, a proprietary protocol or a design that raises the cost of switching may at some point cease to protect users and begin to exclude rivals, and the law needs a principled means of locating that point without either surrendering to the dominant firm's technical authority or substituting a regulator's untested judgment for the engineering knowledge on which genuine security depends. The article approaches the problem by treating cybersecurity as a question of market power. A firm that controls the interfaces through which security is defined, certified and enforced also controls the terms on which others may build, connect and compete, so that its security decisions allocate market opportunity as surely as its pricing decisions do.

Ghana offers an instructive and largely unexamined setting for this inquiry. The country has no general competition statute: a Competition Bill first prepared in 2005 and 2006 has never been enacted, and the Government indicated in its Budget Statement for the 2026 financial year that it intends to submit new consumer protection and competition legislation.[4] Ghanaian law is nonetheless far from silent on competition. The National Communications Authority may classify a network operator or service provider as dominant, may impose corrective obligations on an operator with significant market power, and may require such an operator to make technical information available to other operators.[5] The Authority exercised those powers in June 2020 when it declared Scancom PLC (MTN Ghana) to have significant market power, and in September 2020 the Commercial Division of the High Court dismissed MTN's challenge to that designation.[6] The Bank of Ghana regulates a payment ecosystem whose national mobile money interoperability platform, launched in May 2018, turned a market of closed wallets into one in which value moves across networks, bank accounts and the e-zwich system.[7] The Cyber Security Authority, established by Act 1038, designates and regulates critical information infrastructure and licenses cybersecurity service providers.[8] In its telecommunications and payments sectors, therefore, Ghana already confronts the collision between security mandates and competitive access that larger jurisdictions are now litigating in relation to mobile operating systems.

The argument proceeds in eleven further parts. Part II sets out the economics of digital dependence and explains why security restrictions have particular exclusionary potential in markets characterized by switching costs and network effects. Part III maps the Ghanaian legal framework, and Part IV examines selected foreign regimes. Part V offers a typology of security-justified restraints, on which Part VI builds the Security Necessity and Symmetry Test. Part VII addresses the allocation of evidential burdens and the handling of confidential security material, and Part VIII considers regulatory competence and institutional design. Part IX answers the objection that the test might weaken genuine security, Part X identifies the article's contribution to existing scholarship, and Part XI proposes judicial, regulatory and legislative reforms before Part XII concludes. The method is doctrinal and comparative, supplemented by the published findings of competition authorities and by the transaction data of Ghanaian payment institutions; where the status of a development remains uncertain, the uncertainty is acknowledged rather than resolved by assumption.

II. THE ECONOMICS OF DIGITAL DEPENDENCE

A. Switching costs, network effects and the value of control

The economic literature on lock-in begins from a straightforward observation. A customer who has invested in learning a system, accumulated data within it, bought complementary products for it or built relationships that run through it faces a cost of switching

[3] Google, announcement of Android developer verification (August 2025), under which verification opened to all developers in March 2026, enforcement began in Brazil, Indonesia, Singapore and Thailand on 30 September 2026 and global expansion is planned from 2027; see also the subsequent introduction of an advanced installation flow for experienced users.

[4] LexisNexis, 'Ghana competition and merger control' (Practical Guidance, 2026); CUTS International West Africa, statement on the Consumer Protection and Competition Bills (Accra, 5 December 2025).

[5] Electronic Communications Act 2008 (Act 775), s 20, as amended by the Electronic Communications (Amendment) Act 2016 (Act 910); National Communications Authority Act 2008 (Act 769), s 3.

[6] National Communications Authority, 'NCA Declares MTN as a Significant Market Power' (Press Release, 9 June 2020); National Communications Authority, 'High Court Dismisses MTN's Case Contesting the NCA's Decision to Declare Them as a SMP in Ghana' (1 September 2020).

[7] Ernest Addison, Governor of the Bank of Ghana, speech at the launch of Mobile Money Interoperability Phase II (GhIPSS, Accra, 28 November 2018).

[8] Cybersecurity Act 2020 (Act 1038), ss 2 to 4, 35 to 41, 49 to 59 and 92.

that includes not only the price of the rival product but also the loss of everything that cannot be carried across.[9] Farrell and Klemperer show that switching costs and network effects tend to turn competition within a market into competition for the market, that firms compete aggressively to build an installed base which they later exploit, and that the resulting equilibrium can sustain both supra-competitive prices and the persistence of inferior standards.[10] Digital platforms intensify each of these features. An operating system or a payment network is valuable to a user in proportion to the applications, devices, merchants and counterparties connected to it, and valuable to a developer or merchant in proportion to the users it reaches, so that whoever controls the interface between the two sides can levy a toll on every transaction that crosses it.

Interoperability is the economic counterweight to that control. Where a rival application, device or service can connect to a platform on equivalent terms, the platform owner must compete on the merits of its own complementary products; where it cannot, the platform owner may extend its dominance into adjacent markets and raise the cost of leaving the platform altogether, because a user who switches must abandon not only the platform but every complement that works only with it. The designation decisions adopted by the Competition and Markets Authority in October 2025 illustrate the point. Having found that between 90 and 100 per cent of mobile devices in the United Kingdom run on Apple's or Google's platform, the CMA concluded that users are unlikely to switch between the two and that businesses wishing to reach both populations of users must develop and distribute their products through both.[11] Such is the condition of digital dependence: the dependent party cannot discipline the platform by leaving it, because leaving is not a realistic option.

B. Why security restrictions are distinctive instruments of exclusion

Among the instruments available to a firm in that position, security restrictions are distinctive for four reasons. They are, first, difficult to observe: a price increase is visible and comparable, whereas a decision to deny a rival access to an interface, to classify a category of application as unsafe, or to delay the publication of a technical specification is usually invisible to consumers and opaque to regulators. They are, secondly, difficult to evaluate, since whether a particular access arrangement enlarges the attack surface of a system, and by how much, depends on architectural knowledge that the platform owner possesses and outsiders lack. Thirdly, they enjoy normative prestige, for a firm that restricts access in order to protect users presents itself as a responsible steward, while a regulator or claimant who challenges the restriction risks appearing indifferent to fraud, malware and intrusion by hostile states. Fourthly, security and exclusion are frequently produced by the same act: a closed interface may genuinely reduce some risks while also foreclosing rivals, and the firm that adopts it may sincerely value both effects.

The fourth point is the most important for legal analysis. Security engineering has long accepted that the security of a system should not depend on the secrecy of its design. Kerckhoffs stated the principle for cryptographic systems in 1883, and contemporary practice holds that well-designed systems remain secure even when their mechanisms are known, relying instead on the protection of keys, the isolation of components, the verification of code and the monitoring of behaviour.[12] A claim that security requires the wholesale exclusion of third parties, as distinct from conditioning their access on verifiable safeguards, is therefore a claim that should be examined rather than assumed. That is not to say that every restriction is pretextual. Sandboxing, code signing, permission models, application review and the hardening of critical infrastructure against unauthorized connection are genuine controls of established value, and the legal difficulty consists in separating those controls from the commercial choices that accompany them.

C. The empirical record

The most reliable evidence comes from competition authorities and executive agencies that have examined these questions with compulsory powers or extensive public consultation. In February 2023, the National Telecommunications and Information Administration of the United States Department of Commerce reported, after an inquiry that attracted more than 150 public submissions, that means of distributing applications other than the two dominant mobile stores are possible but face significant barriers to meaningful competition, and it recommended that legislative and regulatory measures prohibit restrictions on sideloading, alternative app stores and web applications while preserving appropriate latitude for privacy and security safeguards.[13] The report did not discount security, which it described as an obvious and pressing need; its conclusion was that the benefits of the existing

[9] Joseph Farrell and Paul Klemperer, 'Coordination and Lock-In: Competition with Switching Costs and Network Effects' in Mark Armstrong and Robert Porter (eds), *Handbook of Industrial Organization*, vol 3 (Elsevier 2007) 1967.

[10] Farrell and Klemperer (n 9); see also Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition Policy for the Digital Era* (Publications Office of the European Union 2019).

[11] Competition and Markets Authority, 'CMA confirms Apple and Google have strategic market status in mobile platforms' (Press Release, 22 October 2025).

[12] Auguste Kerckhoffs, 'La cryptographie militaire' (1883) 9 Journal des sciences militaires 5; Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd edn, Wiley 2020).

[13] National Telecommunications and Information Administration, *Competition in the Mobile Application Ecosystem* (US Department of Commerce, February 2023).

restrictions did not justify their competitive costs and that privacy and security could be protected by less restrictive means.[14] The CMA's 2022 market study of mobile ecosystems reached comparable conclusions about the scope of the security justifications advanced for restrictions on browser engines and app distribution, and those findings informed the strategic market status designations of October 2025.[15]

Ghana's payments history supplies a natural experiment pointing in the opposite direction. Before May 2018, a mobile money customer could not transfer value directly to a wallet held on a rival network. The Bank of Ghana and the Ghana Interbank Payment and Settlement Systems (GhIPSS) then built, with a reported loan of 4.5 million US dollars from the central bank, a switch that connected the mobile money platforms with bank accounts, and later with the e-zwich system.[16] Interoperable transfers rose from 96,907 transactions worth GH¢8.3 million in May 2018 to 319,094 transactions worth GH¢32.6 million by the following September, and GhIPSS recorded 2.2 million interoperable transactions for the period from May to December 2018 and 9.4 million, worth GH¢781.6 million, for 2019.[17] Throughout this period, the Bank of Ghana treated security and the integrity of the payment system as preconditions of interoperability rather than as reasons against it. The lesson is not that interoperability is costless. It is that a regulator with the technical competence to specify the terms of access, and the legal authority to require it, can open the network of a dominant firm without compromising its security, and that the economic gains from doing so may be considerable.

III. THE GHANAIAN LEGAL FRAMEWORK

A. Constitutional foundations

A Ghanaian analysis must begin with the 1992 Constitution, which supplies both the substantive values that competition law serves and the procedural discipline to which every regulator is subject. Among the Directive Principles of State Policy, article 36(2) commits the State to an economic order that affords ample opportunity for individual initiative and creativity, fosters an enabling environment for a pronounced role of the private sector and promotes efficient and productive enterprise.[18] The Supreme Court has held the Directive Principles to be presumptively justiciable and, at the least, authoritative guides to the construction of statutes and the exercise of public power, so that they bear directly on how sectoral regulators should understand their competition mandates.[19] More directly enforceable are article 23, which requires administrative bodies and officials to act fairly and reasonably and to comply with the requirements imposed on them by law, and article 296, which requires discretionary power to be exercised fairly and candidly, without arbitrariness, caprice or bias, and in accordance with published regulations where the Constitution or another law so requires.[20] These provisions operate in two directions. They constrain a regulator that orders a dominant firm to open its systems, because such an order must be reasoned, proportionate and procedurally fair; and they equally constrain a regulator that accepts a dominant firm's security justification without inquiry, because a decision that ignores relevant evidence of exclusion is no less arbitrary than one that ignores relevant evidence of risk.

B. The absent general statute and the regional overlay

Ghana has neither an overarching competition statute nor a general merger control regime, and competition is advanced instead through sector-specific legislation and regulators.[21] Outside telecommunications and payments, the most significant statutory competition provisions are found in the downstream petroleum regime under the National Petroleum Authority Act 2005 (Act 691), and civil society organizations have repeatedly pointed out that Ghanaian law contains no general prohibition of cartel conduct beyond that sector.[22] The Protection Against Unfair Competition Act 2000 (Act 589) deals with confusion, damage to goodwill, misleading conduct and the unauthorized disclosure of secret information, but it regulates unfair practices between traders rather than exclusionary conduct by dominant firms and contains no doctrine of abuse.[23]

At the regional level, ECOWAS has adopted Supplementary Act A/SA.1/12/08 on the Community Competition Rules and Supplementary Act A/SA.2/12/08 establishing the ECOWAS Regional Competition Authority, although practitioners have noted

[14] NTIA (n 13).
[15] Competition and Markets Authority, *Mobile Ecosystems Market Study: Final Report* (10 June 2022).
[16] Citi Business News, report of the statement by the Chief Executive of GhIPSS on the financing of the interoperability platform (May 2018); Citi Business News, report that Phase One was launched on 10 May 2018, connecting the mobile money platforms to the gh-link switch.
[17] Addison (n 7); GhIPSS, 'Mobile Money Interoperability ends 2018 with 2.2 million transactions' (January 2019); MyJoyOnline, 'Mobile Money Interoperability records 267% growth in value' (2020), reporting the GhIPSS summary report for 2019.
[18] Constitution of the Republic of Ghana 1992, art 36(2).
[19] *Ghana Lotto Operators Association v National Lottery Authority* [2007-2008] SCGLR 1088.
[20] Constitution 1992, arts 23 and 296.
[21] LexisNexis (n 4).
[22] National Petroleum Authority Act 2005 (Act 691); CUTS International West Africa (n 4).
[23] Protection Against Unfair Competition Act 2000 (Act 589).

continuing uncertainty about the application of those rules in Ghana because Parliament has not ratified the relevant instruments.[24] At the continental level, the Protocol to the Agreement Establishing the African Continental Free Trade Area on Competition Policy, adopted by the Assembly of the African Union on 19 February 2023, prohibits the abuse of a dominant position and, in a provision of particular relevance to digital markets, the abuse of economic dependence, including obligations for designated digital platforms that apply without proof of dominance.[25] The Protocol enters into force thirty days after the deposit of the twenty-second instrument of ratification and was not in force at the time of writing.[26] Its significance is twofold: it commits State Parties, including Ghana, to the establishment of a functioning national competition regime, and it signals a continental preference for treating economic dependence, and not dominance alone, as a trigger for platform obligations.

C. Telecommunications: significant market power and the duty to share technical information

The most developed competition machinery in Ghanaian law is found in the electronic communications sector. Section 3 of the National Communications Authority Act 2008 (Act 769) charges the Authority with ensuring fair competition among licensees, operators of communications networks and service providers, and the Electronic Communications Act 2008 (Act 775) gives that mandate operational content.[27] Under Act 775, the Authority may classify a network operator or service provider as dominant where, individually or jointly with others, it enjoys a position of economic strength that enables it to behave to an appreciable extent independently of competitors and consumers; it may impose corrective obligations on an operator so classified; and it may regulate prices where there is a sole operator or an operator with significant market power, or where it detects anti-competitive pricing.[28] Licences may also contain conditions prohibiting anti-competitive conduct by the licensee. Of particular importance for present purposes, section 20 obliges an operator with significant market power to make available to other network operators and service providers technical information regarding its network or service, including planned deployments of equipment and other information relevant to those operators.[29] Ghanaian law thus already contains, in a sectoral statute, an obligation to share interoperability information of the kind that European law imposed on Microsoft only after years of litigation.

The 2020 designation of MTN shows the regime at work. Applying the 40 per cent threshold set by the National Telecommunications Policy 2005 and acting under section 20 of Act 775, the Authority found that MTN held more than 57 per cent of the voice market and a larger share of the data market, and it announced corrective measures that included asymmetric interconnection rates and tariff controls.[30] MTN challenged the decision on the ground that it had been denied a fair hearing, and the Commercial Division of the High Court held that there was sufficient evidence of consultation and that the Authority had not acted contrary to law.[31] The designation did not address, and the regime has not yet been asked to address, the treatment of refusals of access justified on security grounds. As mobile networks become platforms for payments, identity and application services, the question whether an operator with significant market power may refuse a rival access to an interface, an application programming interface or a network function on security grounds is bound to arise, and section 20 supplies the statutory basis for answering it. Disputes may be referred to the Electronic Communications Tribunal established under sections 88 to 92 of Act 775, a specialist forum capable of developing the technical jurisprudence that ordinary courts find difficult to build.[32]

D. Payments: interoperability as regulatory policy

The Payment Systems and Services Act 2019 (Act 987) entrusts the Bank of Ghana with the regulation and oversight of payment systems and expressly recognises the facilitation of interoperability of payment systems and services among providers as a licensable service.[33] The Bank may issue rules and guidelines for the implementation of the Act, a power it has used, for example, to regulate the domestic processing of card transactions.[34] Act 987 contains no general prohibition of abuse of dominance, but its licensing, oversight and rule-making powers together give the Bank the means to require access on specified terms, as the mobile money interoperability programme demonstrated. Security lies at the centre of that regime. Because the Bank also oversees the resilience

[24] Supplementary Act A/SA.1/12/08 adopting Community Competition Rules and the Modalities of their Application within ECOWAS; Supplementary Act A/SA.2/12/08 on the Establishment, Functions and Functioning of the ECOWAS Regional Competition Authority; Legal 500, 'Ghana's Corporate Commercial Outlook 2026' (2026).

[25] Protocol to the Agreement Establishing the African Continental Free Trade Area on Competition Policy (adopted 19 February 2023), arts 9 and 11.

[26] AfCFTA Protocol (n 25); tralac, 'AfCFTA Protocol on Competition Policy: Factsheet' (October 2023).

[27] Act 769, s 3.

[28] Act 775, ss 20, 25 and 101 (definition of significant market power).

[29] Act 775, s 20. The text of this provision should be read in its form as amended by Act 910.

[30] NCA, Press Release (n 6); National Communications Authority, 'Public Information: What SMP Means' (19 June 2023).

[31] NCA, 'High Court Dismisses MTN's Case' (n 6).

[32] Act 775, ss 88 to 92.

[33] Payment Systems and Services Act 2019 (Act 987), ss 3 and 7(2)(f).

[34] Act 987, s 101; Bank of Ghana, Guidelines for Domestic Processing of Payment Card Transactions, issued under s 101(2).

of payment systems and has issued its Cyber and Information Security Directive, any refusal of access by a dominant payment provider is likely to be expressed in security terms, and the Bank is the body best placed to evaluate such claims within its sector.[35]

E. Cybersecurity regulation as a source of market structure

The Cybersecurity Act 2020 (Act 1038) is not a competition statute, but it shapes market structure in ways that competition analysis cannot ignore. It establishes the Cyber Security Authority; empowers it to designate and register critical information infrastructure, to audit compliance and to issue directives to the owners of such infrastructure; and requires the licensing of cybersecurity service providers and the accreditation of cybersecurity establishments and professionals.[36] These powers operate as gateways. A directive requiring a designated institution to engage only providers holding a licence of a specified tier raises security standards and at the same time determines which firms may compete for public cybersecurity work, as the administrative penalty of GH¢240,000 imposed in August 2026 on the Office of the Registrar of Companies for engaging an unlicensed provider illustrates.[37] The Data Protection Act 2012 (Act 843), which requires data controllers to adopt appropriate technical and organizational measures to secure personal data, operates in a similar way, because it supplies a ready justification for restricting data portability and access by third parties.[38] Neither statute directs its regulator to consider competitive effects, and that silence is one of the gaps the proposals in this article seek to fill.

IV. COMPARATIVE REGIMES

A. The European Union: from indispensability to the duty to build a template

European law on refusals to deal developed around a demanding test. In *Bronner,* the Court of Justice held that a dominant firm's refusal to grant access to its facility is abusive only where access is indispensable to the requesting firm's business, in the sense that no actual or potential substitute exists, where the refusal is likely to eliminate all competition, and where it is not objectively justified.[39] *IMS Health* added, for refusals to license intellectual property, the requirement that the refusal prevent the emergence of a new product for which there is potential consumer demand.[40] In *Microsoft,* the Court of First Instance applied that framework to interoperability information for work group server operating systems, upheld the Commission's finding of abuse and rejected Microsoft's objective justification because Microsoft had not shown that disclosure would significantly reduce its incentives to innovate, observing that the disclosure of interoperability information was common in the software industry.[41] Two features of the judgment deserve emphasis: the burden of establishing the justification lay on the dominant firm, and the Court required that the justification be substantiated with specific evidence rather than asserted at a level of generality that would have deprived the refusal doctrine of effect.

The leading modern authority is *Alphabet v AGCM*, decided on 25 February 2025.[42] Google had developed Android Auto as a platform open to third-party developers through templates, but it refused to develop a template for Enel X's JuicePass application, citing security concerns and the allocation of development resources. The Court held that the *Bronner* condition of indispensability does not apply where the dominant firm has developed a platform not solely for its own use but with a view to enabling third parties to use it; that a refusal may be abusive even if the requesting firm and its competitors continue to operate and grow without interoperability; and that a refusal may be justified where no template exists for the category of application concerned and the grant of interoperability would compromise the security or integrity of the platform, or where interoperability is impossible for other technical reasons. In the absence of such a justification, the dominant firm must develop a template within a reasonable period, in return for appropriate financial compensation.[43] The judgment reframes the security question. Security no longer ends the inquiry; it becomes a defence that must be shown to apply to the specific access requested, and if it fails, the dominant firm's position changes from a right to refuse into a duty to build.

On 2 July 2026, the Court of Justice dismissed Google's appeal in *Google Android*, confirming a fine of approximately €4.1 billion for restrictions imposed on device manufacturers and network operators in connection with the Android ecosystem.[44] Although the

[35] Bank of Ghana, Cyber and Information Security Directive (2018).
[36] Act 1038 (n 8).
[37] Ghana News Agency, 'CSA fines ORC GH¢240,000 over cybersecurity non-compliance' (13 August 2026).
[38] Data Protection Act 2012 (Act 843), s 28.
[39] Case C-7/97 *Oscar Bronner GmbH & Co KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co KG* [1998] ECR I-7791.
[40] Case C-418/01 *IMS Health GmbH & Co OHG v NDC Health GmbH & Co KG* [2004] ECR I-5039.
[41] Case T-201/04 *Microsoft Corp v Commission* [2007] ECR II-3601.
[42] *Alphabet v AGCM* (n 1).
[43] ibid.
[44] Case C-738/22 P *Google LLC and Alphabet Inc v Commission* (CJEU, 2 July 2026), dismissing the appeal against Case T-604/18 *Google and Alphabet v Commission (Google Android)* (General Court, 14 September 2022).

case concerned contractual tying and exclusivity rather than security, it confirms that the ecosystem as a whole, and not only its individual products, is the proper unit of competitive analysis, and that control of a mobile platform can be used to entrench adjacent services.

The Digital Markets Act moves from adjudication to regulation. Article 6(7) requires designated gatekeepers to allow providers of services and hardware free and effective interoperability with, and access for interoperability to, the same operating system, hardware and software features as are available to the gatekeeper's own services, while permitting measures to ensure that interoperability does not compromise the integrity of those features, provided that such measures are strictly necessary and proportionate and are duly justified by the gatekeeper.[45] Articles 6(4), on alternative app distribution, and 7, on the interoperability of messaging services, contain parallel integrity and security clauses expressed in the same terms.[46] On 19 March 2025, the Commission adopted its first specification decisions under article 8(2), setting out the measures Apple must take to open nine iOS connectivity features to third-party connected devices such as smartwatches and headphones, and to improve its process for handling interoperability requests.[47] The Digital Markets Act provides the closest existing legislative model for the test proposed in Part VI. Its limitation, from the perspective of a jurisdiction such as Ghana, is that it applies only to a small number of designated gatekeepers and relies on an enforcement apparatus of a scale that no African regulator possesses.

B. The United States: the rule of reason and the burden of proving alternatives

United States law addresses the same problem through the prohibition of monopolization in section 2 of the Sherman Act and the rule of reason under section 1. *United States v Microsoft* remains the leading treatment of technological design as exclusionary conduct. The en banc District of Columbia Circuit held that product design decisions are not immune from scrutiny, that a monopolist may offer a procompetitive justification for conduct shown to have anticompetitive effects, and that the plaintiff may then rebut the justification or show that the harm outweighs the benefit; it rejected several of Microsoft's technical justifications for want of supporting evidence.[48] The Supreme Court's decisions in *Aspen Skiing* and *Trinko* confine liability for refusals to deal with rivals to narrow circumstances, and *Trinko* cautioned expressly against compelled sharing that would require courts to act as central planners.[49]

Epic Games v. Apple demonstrates how much depends on the allocation of the burden of identifying less restrictive alternatives. The Ninth Circuit accepted that Apple's restrictions had anticompetitive effects, but held that Apple had established non-pretextual procompetitive rationales, including improvements in device security and user privacy that differentiated iOS from its rivals, and that Epic had failed to prove substantially less restrictive alternatives capable of achieving those ends.[50] The decision is often read as a vindication of security justifications, but it is better understood as a lesson in evidential architecture: the plaintiff lost because it bore the burden of proving an alternative whose feasibility depended largely on information under the defendant's control.[51] The contrast with the monopolization action brought by the Department of Justice and a group of States in March 2024 is instructive. That action alleges that Apple uses restrictions on super apps, cloud streaming, cross-platform messaging, third-party smartwatches and digital wallets to make switching between smartphones more difficult, and on 30 June 2025 the District Court for the District of New Jersey denied Apple's motion to dismiss, treating Apple's contention that it may design its platform to prioritize security, privacy and user experience as a factual matter unsuitable for resolution on the pleadings.[52]

C. The United Kingdom: designation and conduct requirements

The Digital Markets, Competition and Consumers Act 2024 authorizes the CMA to designate a firm as having strategic market status where it has substantial and entrenched market power and a position of strategic significance in a digital activity, and to impose tailored conduct requirements on it.[53] On 22 October 2025, the CMA designated Apple and Google as having strategic market status in their mobile platforms for a period of five years. Its published roadmaps identified the fair consideration of

[45] 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) [2022] OJ L265/1, art 6(7) and recital 50.

[46] DMA (n 45), arts 6(4) and 7.

[47] Commission Implementing Decision of 19 March 2025, Case DMA.100203, Article 6(7), Apple, iOS, Features for Connected Physical Devices, C(2025) 3000, summary at OJ C/2025/4646; Commission Implementing Decision of 19 March 2025, Case DMA.100204 (process for interoperability requests).

[48] *United States v Microsoft Corp* 253 F 3d 34 (DC Cir 2001) (en banc).

[49] *Aspen Skiing Co v Aspen Highlands Skiing Corp* 472 US 585 (1985); *Verizon Communications Inc v Law Offices of Curtis V Trinko LLP* 540 US 398 (2004).

[50] *Epic Games v Apple* (n 2).

[51] ibid; see the questions presented in Epic's petition for certiorari, *Epic Games Inc v Apple Inc*, No 23-337 (filed 27 September 2023), concerning the test for a less restrictive alternative.

[52] *United States v Apple Inc*, No 2:24-cv-04055 (D NJ, 30 June 2025) (order denying motion to dismiss).

[53] Digital Markets, Competition and Consumers Act 2024.

interoperability requests, app review and steering as early priorities, and it has since secured commitments from both firms on the fairness of app review and on iOS interoperability.[54] The British model is instructive because it situates the security inquiry within an iterative regulatory relationship rather than a single adversarial contest, enabling the regulator to test security claims through a succession of specific requests.

D. African regimes

South Africa's Competition Act 89 of 1998 offers the most developed African model of a structured justification. Section 8 prohibits a dominant firm from refusing a competitor access to an essential facility and prohibits specified exclusionary acts unless the firm can show technological, efficiency, or other procompetitive gains that outweigh the anticompetitive effect.[55] The statutory language places the burden of establishing the countervailing gain squarely on the dominant firm, which is the allocation defended in this article. Kenya's Competition Act 2010 prohibits abuse of a dominant position in section 24, and Nigeria's Federal Competition and Consumer Protection Act 2018 contains equivalent provisions.[56] None of these regimes contains a justification clause specific to security, and none has yet produced a reported decision squarely concerned with a refusal of interoperability on security grounds. The field is therefore open for a Ghanaian contribution of continental relevance, particularly as the provisions of the AfCFTA Protocol on abuse of economic dependence approach entry into force.

V. WHEN SECURITY BECOMES EXCLUSION: A TYPOLOGY

The comparative material shows that security-justified restraints do not constitute a single category of conduct. They take at least six recurring forms, and a test that treated them identically would be too permissive for some and too intrusive for others. The typology that follows is an analytical device, and its Ghanaian illustrations describe plausible applications of existing statutory powers rather than findings about the conduct of any particular firm.

Outright refusal of access. The simplest form is the refusal to open an interface, a network function or an application programming interface to a rival, as in *Alphabet v AGCM*. Its Ghanaian equivalent would be a refusal by an operator with significant market power to give a financial technology provider access to a network channel, or a refusal by a dominant wallet provider to give a rival access to an integration point used by its own affiliated services. The exclusionary potential of such conduct is greatest where the platform was designed to host third parties, and the refusal is selective.

Conditional access on disproportionate terms. More common, and more difficult to assess, is access granted on conditions whose security value is real but whose burden falls unevenly. Certification requirements, identity verification for developers, mandatory audits by approved assessors and review processes of indeterminate duration all belong to this category. Google's developer verification programme is a current example, presented as a means of deterring the distribution of malware but criticized as raising the cost of independent distribution while doing little to obstruct the methods that sophisticated attackers employ.[57] The legal question is not whether verification has any security value, which it may well have, but whether its scope, cost and administration are proportionate to that value.

Degradation of interoperability. A firm may permit nominal access while ensuring that rival products perform less well than its own, through delayed notifications, restrictions on background operation, limited access to sensors or connectivity features, or encryption and authentication confined to its own devices. The Department of Justice's allegations concerning third-party smartwatches and cross-platform messaging are of this kind.[58] Degradation is especially insidious because it raises switching costs without any visible refusal and allows the firm to attribute an inferior experience to the deficiencies of the rival's product.

Proprietary protocols and component pairing. A firm may encrypt or authenticate the communications between its system and complementary products so that only authorised components, accessories or replacement parts will function. Authentication of this kind can protect users against counterfeit and dangerous components, but it can equally extinguish independent markets for compatible products and repair services. The law must therefore distinguish authentication that verifies safety properties from authentication that verifies nothing more than commercial affiliation.

Security-justified enclosure of data. Data protection and security obligations, including those arising under section 28 of Act 843, may be invoked to refuse data portability or access by a third party to customer data that a rival needs to compete. In such cases, the security justification often coincides with a genuine legal duty, and the question becomes whether that duty requires refusal or merely requires that access be conditioned on consent, authentication and data minimization.

---

[54] CMA (n 11); Competition and Markets Authority, 'The CMA's programme of work across mobile platforms' (guidance, updated 2026).

[55] Competition Act 89 of 1998 (South Africa), s 8.

[56] Competition Act 2010 (Kenya), s 24; Federal Competition and Consumer Protection Act 2018 (Nigeria), ss 70 to 72.

[57] See the announcement cited at (n 3) and the public objections of the F-Droid project and the Keep Android Open campaign (2025 and 2026).

[58] *United States v Apple* (n 52).

Capture of the security standard. An incumbent may, finally, influence the standards, licensing tiers or procurement criteria by which security is measured, so that the regulatory definition of a secure provider comes to coincide with the incumbent's own architecture. The tiered licensing of cybersecurity service providers under Act 1038, and directives requiring owners of critical information infrastructure to engage only providers of a specified tier, are legitimate instruments of national security policy; they also determine market entry, and they should be designed and periodically reviewed with that effect in mind.[59]

One diagnostic recurs across all six forms, namely the treatment of the dominant firm's own services. A restriction that applies equally to the firm's affiliated products and to those of its rivals is more likely to reflect a genuine security judgment, because the firm itself bears its cost. A restriction from which the firm's own services are exempt, or which those services satisfy through privileged channels unavailable to others, is one whose security rationale the firm has itself declined to accept. That asymmetry provides the foundation for the test developed in the next Part.

VI. THE SECURITY NECESSITY AND SYMMETRY TEST

A. Design principles

A defensible test must satisfy four requirements. It must be capable of administration by a Ghanaian court, tribunal or sectoral regulator without the investigative resources of the European Commission. It must respect the engineering reality that some risks justify exclusion and that security choices made in good faith deserve a margin of appreciation. It must neutralize the informational advantage that otherwise allows a dominant firm to prevail by assertion. And it must yield remedies that preserve security rather than forcing a choice between complete closure and unconditioned openness. The Security Necessity and Symmetry Test is constructed around those requirements. It takes its structure from the doctrine of objective justification applied in *Microsoft* and *Alphabet v AGCM*, its language of necessity and proportionality from article 6(7) of the Digital Markets Act and section 8 of the South African Competition Act, and its allocation of burdens from the Evidence Act 1975, while adding two elements that none of those sources state expressly, namely symmetry and contemporaneity.

B. The seven stages

The table below summarizes the seven stages of the test, the question each poses, the party bearing the burden and the consequence of failure at that stage. The commentary that follows explains each stage in turn.

Stage	Question	Burden	Consequence of failure
1. Dependence	Does the firm hold dominance, significant market power or a position on which the complainant is economically dependent?	Complainant or regulator	The test does not apply and ordinary commercial freedom governs.
2. Restraint and capability of foreclosure	Does the conduct restrict access, interoperability or switching in a manner capable of hindering competition in a related market or entrenching the platform?	Complainant or regulator	There is no case to answer.
3. Particularised and contemporaneous security claim	Has the firm identified the asset protected, the threat and the mechanism by which the restraint reduces it, and did that rationale exist when the restraint was adopted?	Dominant firm (persuasion)	The justification fails and the restraint is treated as unjustified.
4. Efficacy	Does credible evidence show that the restraint materially reduces the identified risk?	Dominant firm (persuasion)	The justification fails.
5. Symmetry	Does the restraint apply equally to the firm's own and affiliated services?	Complainant shows asymmetry; firm must then explain it	An unexplained asymmetry raises a rebuttable presumption of pretext.
6. Least restrictive alternative that preserves security	Is there a feasible alternative that achieves comparable security with less harm to competition?	Complainant identifies a plausible alternative; firm bears persuasion on its inadequacy	The restraint is disproportionate and access on conditions is ordered.

[59] Act 1038, ss 49 to 59; Ghana News Agency (n 37).

Stage	Question	Burden	Consequence of failure
7. Residual balancing	Do the remaining security benefits outweigh the competitive harm, with severe and irreversible risks weighted more heavily?	Decision maker, on the whole record	The restraint is upheld or modified.

Stage 1: dependence. The test is engaged only where the firm holds market power sufficient to make its restrictions consequential for competition. In Ghana, that threshold is satisfied by a designation of significant market power under section 20 of Act 775, by an equivalent finding by the Bank of Ghana in respect of a payment provider and, once a general statute is enacted, by a finding of dominance under it. The test should also extend to economic dependence in the sense used in article 11 of the AfCFTA Protocol, since a firm that is not dominant in a defined market may nonetheless control a gateway for which particular rivals or business users have no realistic alternative.

Stage 2: restraint and capability of foreclosure. The complainant must show that the conduct restricts access, interoperability or switching and is capable of hindering competition. Following *Alphabet v AGCM*, it should be unnecessary to prove that the requested access is indispensable where the platform was designed to host third parties, or that rivals have been eliminated; it suffices that the conduct is capable of hindering the maintenance or growth of competition.

Stage 3: a particularized and contemporaneous security claim. At this stage the burden passes to the dominant firm, which must identify with specificity the asset the restraint protects, the threat against which it guards and the mechanism by which it reduces that threat. Generic references to malware, fraud or integrity will not suffice, just as the Court of First Instance refused to accept Microsoft's generalized argument about incentives to innovate.[60] The claim must also be contemporaneous, in the sense that the firm should be able to show from documents created when the restraint was adopted that the security rationale was among the reasons for it. A rationale constructed only after a complaint has been made is not necessarily false, but it deserves less weight, because the firm's actual decision-making process is the best evidence of the purpose the restraint was meant to serve.

Stage 4: efficacy. The firm must then show by credible evidence that the restraint materially reduces the identified risk. Credible evidence includes incident data, threat assessments, the findings of independent security researchers, the firm's own practice in other markets or product lines, and the experience of comparable platforms that do not impose the restraint. Where a firm permits on one product line what it forbids on another, as Epic contended Apple did by allowing broader distribution on its desktop computers, the inconsistency is itself evidence bearing on efficacy.[61]

Stage 5: symmetry. Symmetry is the principal innovation of the test. If the complainant shows that the firm's own or affiliated services are exempt from the restraint, or satisfy it through privileged channels unavailable to rivals, the firm must explain the asymmetry by reference to a difference between its services and those of its rivals that is relevant to security. If it cannot do so, the asymmetry raises a rebuttable presumption that the restraint is pretextual. The rationale is that a firm genuinely persuaded of a risk would not expose its own users to that risk through its own services, so that self-exemption reveals the firm's own assessment of the rule's true purpose. Symmetry does not require identical treatment where the firm can show that its own services are subject to equivalent controls, but that equivalence must be demonstrated rather than assumed.

Stage 6: the least restrictive alternative that preserves security. The complainant must identify a plausible alternative, such as conditioned access through a documented and audited interface, certification against a published standard, independent security assessment, graduated access that expands as a rival demonstrates compliance, user-controlled permissions accompanied by informed warnings, or sandboxing. The burden of persuading the decision maker that the alternative is inadequate then lies on the dominant firm, which alone possesses the architectural knowledge needed to evaluate it. This allocation departs deliberately from *Epic Games v Apple*, in which the plaintiff bore the burden of proving a substantially less restrictive alternative and lost largely for that reason. The departure is justified in the case of dominant firms because the usual reason for placing the burden on the plaintiff, namely that the plaintiff seeks to disturb a legitimate private choice, carries less force where the choice belongs to a firm on which others depend, and because Ghanaian evidence law permits the burden to follow the realities of proof, as Part VII explains.

Stage 7: residual balancing. Where a restraint survives the earlier stages, the decision maker weighs its remaining security benefits against its harm to competition. The weighing is not neutral. Risks that are severe, systemic or irreversible, such as the compromise of critical information infrastructure designated under Act 1038 or of the settlement layer of the payment system, carry greater weight, and in those settings a decision maker should be slow to order access that a competent security authority has advised against. Conversely, where the risk is modest, falls principally on users who have chosen to accept it or can be remedied after the event, the competitive harm of continued exclusion will ordinarily prevail.

[60] *Microsoft v Commission* (n 41).
[61] *Epic Games v Apple* (n 2).

C. Remedial consequences

The test does not culminate in a binary choice. A restraint that fails at the third, fourth or fifth stage is unjustified and should be removed, but its removal can, and usually should, take the form of an order for access on conditions that preserve security, consistently with the Court of Justice's requirement in *Alphabet v AGCM* that a template be developed within a reasonable period and for appropriate compensation. A restraint that fails at the sixth stage should be replaced by the alternative identified, and only at the seventh stage does the decision maker uphold or modify the restraint on the balance of benefits and harms. This graduation of remedies is what enables the test to discipline pretext without weakening genuine protection.

VII. EVIDENCE, BURDENS AND CONFIDENTIAL SECURITY MATERIAL

A. The allocation of burdens under Ghanaian law

The Evidence Act 1975 (NRCD 323) distinguishes the burden of persuasion, which obliges a party to establish a requisite degree of belief in the mind of the tribunal of fact, from the burden of producing evidence, which obliges a party to introduce sufficient evidence to avoid a ruling against it on an issue.[62] Section 14 provides that, except as otherwise provided by law, and unless and until it is shifted, a party bears the burden of persuasion as to each fact whose existence or non-existence is essential to the claim or defence that party asserts.[63] In civil proceedings, the standard is ordinarily proof by a preponderance of the probabilities.[64] These provisions correspond closely to the structure of the test. Dependence and the capability of foreclosure are elements of the complainant's claim, on which the complainant bears the burden of persuasion. The security justification is a defence asserted by the dominant firm, so that the facts essential to it, namely the particularized threat, its contemporaneous existence as a reason for the restraint and the restraint's efficacy, must be established by the firm. The allocation proposed in Part VI is accordingly an application of the general rule of Ghanaian evidence law rather than an innovation imposed upon it.

The fifth and sixth stages raise more delicate questions. At the fifth stage, the complainant must produce evidence of asymmetry, which will often be observable from outside the firm; once it has done so, the burden of producing an explanation shifts to the firm, and an unexplained asymmetry supports an inference of pretext that the tribunal is entitled to draw. At the sixth stage, the complainant bears an evidential burden to identify a plausible alternative, but the burden of persuasion as to its inadequacy should rest on the firm. That allocation accords with the long-established common law principle that the burden of proving a fact may be placed on the party with peculiar knowledge of it, a principle to which the opening words of section 14 leave courts free to give effect.[65] In a dispute about whether an alternative interface would compromise the integrity of an operating system or a payment switch, the dominant firm is in every practical sense the party with peculiar knowledge.

B. Disclosure without exposure

The most serious practical objection to requiring dominant firms to substantiate their security claims is that substantiation may itself create risk. A detailed threat model, a description of unremediated weaknesses or an account of how an attacker might exploit a proposed interface is precisely the information an attacker would most wish to obtain, and a process that forced such material onto the public record would weaken security in the very act of testing it. The answer is not to accept unsubstantiated claims but to adopt procedures that permit substantiation without exposure.

Three procedures are available for that purpose. The first is the confidentiality ring, under which sensitive material is disclosed only to named external lawyers and experts who have given undertakings; it is an established feature of competition litigation in the United Kingdom, and of the European Commission's data room practice, and Ghanaian courts may adopt equivalent arrangements in the exercise of their power to regulate their own procedure.[66] The second is the reception of the most sensitive material in camera, with the tribunal giving a closed account of its reasoning on that material and an open judgment on all other matters. The third, and in Ghana the most useful, is reference of the technical question to an expert body. The Cyber Security Authority has statutory functions in respect of critical information infrastructure, incident response and cybersecurity standards, and it is the natural source of an independent technical opinion on whether a claimed risk is real and whether a proposed alternative would contain it.[67] Such an opinion would not bind the tribunal on the competition question, but it would supply the expertise whose absence otherwise forces tribunals to choose between deference and conjecture.

---

[62] Evidence Act 1975 (NRCD 323), ss 10 and 11.

[63] NRCD 323, s 14.

[64] NRCD 323, s 12.

[65] *R v Turner* (1816) 5 M & S 206, 105 ER 1026.

[66] On confidentiality rings, see the Competition Appeal Tribunal Rules 2015 (SI 2015/1648) and the practice of the Competition Appeal Tribunal; on data rooms, European Commission, *Best Practices on the disclosure of information in data rooms in proceedings under Articles 101 and 102 TFEU and under the EU Merger Regulation* (2015).

[67] Act 1038, ss 3, 4 and 35 to 41.

C. The standard of review of regulatory decisions

Where the decision under challenge is that of a regulator, such as an order of the National Communications Authority requiring an operator with significant market power to open an interface or a rule of the Bank of Ghana mandating access to a payment channel, the reviewing court applies the constitutional standards of articles 23 and 296, whether on an application for judicial review under Order 55 of the High Court (Civil Procedure) Rules 2004 (CI 47) or on an appeal by such specialized route as the governing statute provides.[68] The test supplies the structure of that review. A regulator that has required the dominant firm to substantiate its security claim, has considered symmetry and alternatives, and has consulted the Cyber Security Authority will have exercised its discretion fairly and candidly. A regulator that has accepted a generic assertion of security without inquiry, or has ordered unconditioned access without considering the risk, will not have done so.

VIII. REGULATORY COMPETENCE AND INSTITUTIONAL DESIGN

A. The problem of competence

Security-justified restraints lie at the intersection of three bodies of expertise that Ghanaian law has assigned to different institutions. The National Communications Authority and the Bank of Ghana understand the market structures of their sectors and possess the powers to designate market power and to require access. The Cyber Security Authority understands threat environments, critical information infrastructure and the technical meaning of security standards. The courts, and in the communications sector the Electronic Communications Tribunal, are expert in legality, procedural fairness and the evaluation of evidence. None of these institutions is competent on its own to decide whether a particular security restriction is necessary and proportionate, and the danger of the present arrangement is that each may defer to the others in a manner that leaves the dominant firm's assertion effectively unreviewed.

The problem has two modes of failure. In the first, a regulator focused on competition orders access without adequately understanding the risk, and the resulting interface becomes a channel for fraud or intrusion, at a reputational cost that would set back the cause of interoperability for years. In the second, a regulator focused on security accepts the dominant firm's characterisation of risk because it lacks the economic tools to perceive the exclusionary effect, and thereby lends public authority to private foreclosure. European experience also illustrates the limits of institutional innovation: in *Microsoft* the Court of First Instance annulled the provision of the Commission's decision establishing a monitoring trustee, on the ground that the Commission could not lawfully confer on the trustee powers it did not itself possess or impose on Microsoft the cost of the arrangement.[69] Institutional design must remain within the legal competence of the body that adopts it.

B. A structured institutional pairing

The solution proposed here is a structured pairing of existing institutions rather than the creation of a new one. Where a sectoral regulator or a court is asked to evaluate a security-justified restraint imposed by a firm with significant market power, it should obtain a written technical opinion from the Cyber Security Authority on the third, fourth and sixth stages of the test, that is, on whether the claimed threat is real, whether the restraint materially reduces it and whether the proposed alternative would contain it. The Authority's opinion would be confined to security. The competition questions arising at the first, second, fifth and seventh stages would remain for the competition decision maker, which would be required to give substantial weight to the Authority's opinion on technical matters and to give reasons for any departure from it. This division respects the comparative advantage of each institution and produces a record that a reviewing court can examine under articles 23 and 296.

The pairing should operate in both directions. Where the Cyber Security Authority proposes a directive or standard that would determine market access, such as a tiered licensing requirement or a mandatory architecture for critical information infrastructure, it should consult the relevant sectoral regulator and, once one is established, the national competition authority, on the competitive effects of the measure and on whether a less restrictive measure would achieve the same security objective. Security regulation that disregards competition may produce the very concentration that makes systems fragile, since a market dependent on a single provider or architecture is a market with a single point of failure.

C. Instruments of coordination available now

Nothing in Ghanaian law prevents these arrangements from being introduced immediately through a memorandum of understanding among the National Communications Authority, the Bank of Ghana and the Cyber Security Authority, followed by published guidelines. The Authority's duty to ensure fair competition under Act 769, the Bank's powers of oversight and rule-making under Act 987, and the advisory and standard-setting functions of the Cyber Security Authority under Act 1038 together provide a sufficient legal basis.[70] Legislation would strengthen and formalize the arrangement, but the absence of a general competition statute

[68] High Court (Civil Procedure) Rules 2004 (CI 47), Order 55; Constitution 1992 (n 20).
[69] *Microsoft v Commission* (n 41), annulling art 7 of the Commission's decision.
[70] Act 769, s 3; Act 987 (n 33) and s 101; Act 1038, ss 3 and 4.

is no reason for delay. The European Union developed its interoperability jurisprudence for two decades before it enacted the Digital Markets Act, and Ghana's sectoral regulators already hold powers more specific than those on which the European Commission relied in *Microsoft*.

IX. THE RISK OF WEAKENING GENUINE SECURITY: OBJECTIONS AND LIMITS

A. The asymmetry of error costs

The strongest objection to any test that subjects security restrictions to competition scrutiny is that the costs of error are asymmetric. If a court wrongly upholds a pretextual restriction, consumers pay higher prices and rivals lose opportunities, harms that are real but recoverable. If a court wrongly strikes down a genuine restriction, the resulting breach may expose millions of users to fraud, compromise a payment system or disable critical infrastructure, harms that may be neither recoverable nor confined to the parties. The objection carries particular force in Ghana, where mobile money is the principal financial instrument for a large population of users, many of whom are new to digital services and vulnerable to social engineering, and where a successful attack on a dominant network could affect the payment habits of the entire country.

The test accommodates this objection in three ways. The seventh stage gives greater weight to severe, systemic and irreversible risks and counsels restraint where a competent security authority has advised against access. The graduation of remedies means that the ordinary response to an unjustified restraint is conditioned access rather than unconditioned openness. And the institutional pairing described in Part VIII ensures that no order for access is made without an independent technical assessment. The objection would be decisive against a rule that treated security claims with general suspicion, but it has no such force against a rule that requires only that security claims be particularized, contemporaneous, effective, symmetrical and proportionate.

B. Incentives to innovate and invest

A second objection, associated with *Trinko*, holds that compelled access reduces the incentive of the platform owner to invest in its platform and the incentive of rivals to build their own.[71] The objection has empirical content and must be taken seriously, but the evidence from the European interoperability cases and from Ghana's experience of payments suggests that it is weakest where security restrictions are concerned. In *Microsoft,* the Court of First Instance found that the dominant firm had not shown that disclosure would significantly reduce its incentive to innovate. In Ghana, mandated mobile money interoperability was followed not by a collapse of investment but by rapid growth in transaction volumes and by the entry of new services built on the interoperable infrastructure.[72] The test accommodates legitimate concerns about investment at its seventh stage and in the assessment of compensation, since an order to build an interface for a rival may, and ordinarily should, be accompanied by appropriate payment, as *Alphabet v AGCM* recognized.

C. Liability and the reallocation of risk

A third objection concerns liability. If a dominant firm is ordered to open an interface and a rival's product is then used to compromise users, it is unclear who should bear the resulting loss, and in the absence of a clear answer, dominant firms will resist orders for access on grounds of liability even where the security risk is manageable, while regulators will hesitate to make such orders. The answer should be supplied by the order itself. It should specify the security conditions with which the party obtaining access must comply, provide for the suspension of access on credible evidence of a security incident, and allocate to that party liability for losses caused by its breach of those conditions. A dominant firm that complies with an order for access and with its own security obligations should not be liable for losses caused by a third party's breach. That allocation removes the strongest legitimate reason for resistance while leaving the dominant firm responsible for the security of its own systems.

D. Disclosure of vulnerabilities and the security of the process

A fourth objection is that the process of testing security claims may itself disclose exploitable information. Part VII has addressed that concern through confidentiality rings, closed material and reference to the Cyber Security Authority, and one further safeguard should be added. No decision maker should require the public disclosure of an unremediated vulnerability as a condition of accepting a security justification, and a justification that rests on such a vulnerability should be capable of being established before the Cyber Security Authority alone, subject to an open statement of the Authority's conclusion. This safeguard aligns the test with the logic of coordinated vulnerability disclosure, under which the timing of disclosure is managed so as to permit remediation before exposure.

E. The argument from centralized control

It is sometimes argued, finally, that closed and centrally controlled systems are more secure because they present a single, well-defended perimeter. The argument captures a truth about the value of coordinated defence, but it neglects the systemic fragility of

[71] *Trinko* (n 49).

[72] See Part II.C above and the sources cited at (n 17).

dependence. A digital economy in which payments, identity and communications run through the architecture of one or two firms is an economy in which a single failure, whether of security, of operation or of corporate decision, can propagate everywhere. Interoperability on secure terms is not opposed to resilience but is one of its conditions, and a test that disciplines pretextual closure therefore serves national cybersecurity policy as well as competition policy.

X. CONTRIBUTION TO EXISTING SCHOLARSHIP

The literature on digital platforms and competition is now extensive, and this article does not claim to have discovered that platforms possess market power or that interoperability can discipline it. The expert reports commissioned in Europe and the United States in 2019 made the case for interoperability as a remedy for digital dependence, and scholarship in the United States has examined how vertical integration and control of interfaces allow platform owners to entrench adjacent services.[73] Nor is the article the first to observe that privacy and security may be advanced as procompetitive justifications, a theme that runs through the commentary on *Epic Games v. Apple* and the debates surrounding the Digital Markets Act. Its contribution lies in five more specific claims.

The first is a reconception of security as a variable of market power rather than an external constraint on competition law. Existing analysis typically asks whether a security justification outweighs an anticompetitive effect, treating security and competition as separate goods to be balanced against each other. The argument advanced here is that control over the definition and enforcement of security is itself a source of market power, so that the relevant question concerns not only the weight that security deserves but also who decides what security requires and on what evidence.

The second is the symmetry principle, which provides a diagnostic of pretext that does not depend on access to the firm's internal deliberations. Existing tests require courts to identify pretext through evidence of motive or through the balancing of effects, both of which depend heavily on information that the dominant firm controls, whereas self-exemption is observable from outside the firm and reveals its own assessment of the restriction's purpose. To the author's knowledge, no court or legislature has yet articulated symmetry as a distinct stage of the justification inquiry, although the requirement in the Digital Markets Act that gatekeepers give third parties access to the same features as are available to their own services rests on a related intuition.[74]

The third is an allocation of burdens that follows informational control and is grounded in the general rule of the Evidence Act 1975. The comparison with *Epic Games v Apple* shows how decisively the location of the burden on less restrictive alternatives can determine outcomes, and by placing the burden of persuasion as to the inadequacy of a plausible alternative on the party with peculiar knowledge, the test corrects an asymmetry that the rule of reason in the United States leaves in place.

The fourth is a design suited to a jurisdiction without a general competition statute. Much of the existing literature presupposes either a mature antitrust regime or a bespoke statute for digital markets, and Ghana has neither. It does, however, possess sectoral powers over market power, a statutory duty on operators with significant market power to share technical information, a central bank that has already mandated interoperability in payments, and a cybersecurity authority with standard-setting functions. Demonstrating how those instruments can be assembled into a coherent doctrine now, rather than after the enactment of legislation that has been pending for two decades, is of practical value to Ghana and to other African jurisdictions in a comparable position.

The fifth is a reciprocal institutional pairing between security and competition regulators, under which competition decision makers obtain independent technical assessments of security claims and security regulators assess the competitive effects of their own directives. The proposition that security regulation can itself create market structure, so that cybersecurity licensing and directives on critical infrastructure require competition review, remains underdeveloped in both the competition and the cybersecurity literature.

XI. REFORMS

A. Judicial reforms

Courts and the Electronic Communications Tribunal can adopt the test without legislative change, because each of its elements rests on existing law: the constitutional duties of fair and candid decision-making in articles 23 and 296, the rules on the burden of proof in the Evidence Act 1975, and the requirement of fair competition in the sectoral statutes. Four judicial practices would give it effect. First, in reviewing a regulator's decision on a security-justified restraint, courts should ask whether the regulator required the dominant firm to particularize its security claim, examined the contemporaneity and efficacy of that claim, considered symmetry and alternatives, and obtained an independent technical opinion, and should treat a decision that omits these steps as one that has failed to take relevant considerations into account. Secondly, courts should apply section 14 of NRCD 323 so that the facts essential to a security defence must be proved by the party asserting it, and should give effect to the principle of peculiar knowledge in

[73] Crémer, de Montjoye and Schweitzer (n 9); Stigler Committee on Digital Platforms, *Final Report* (George J Stigler Center for the Study of the Economy and the State, University of Chicago Booth School of Business 2019); Herbert Hovenkamp, 'Antitrust and Platform Monopoly' (2021) 130 Yale LJ 1952; Lina M Khan, 'Amazon's Antitrust Paradox' (2017) 126 Yale LJ 710.

[74] DMA (n 45), art 6(7).

allocating the burden of persuasion as to the adequacy of alternatives. Thirdly, courts should develop, in the exercise of their power to regulate their own procedure, confidentiality rings and closed material procedures for security evidence, and should publish guidance so that parties can plan disclosure. Fourthly, where a restraint is found to be unjustified, courts and the Tribunal should prefer orders for conditioned access, specifying security conditions, a mechanism for suspension and an allocation of liability, to orders for unconditioned openness.

B. Regulatory reforms

The sectoral regulators can act immediately through guidelines and memoranda of understanding. The National Communications Authority should issue guidelines under its mandate to ensure fair competition, explaining how it will apply section 20 of Act 775 to refusals of access, and to conditions of access that operators with significant market power justify on security grounds, and adopting the test as its analytical framework. The Bank of Ghana should extend its interoperability policy from settlement infrastructure to application programming interfaces, publishing technical and security standards for access by third parties to payment accounts and requiring dominant providers to give reasons, by reference to those standards, for any refusal.

The National Communications Authority, the Bank of Ghana and the Cyber Security Authority should also conclude a memorandum of understanding establishing the procedure for technical opinions described in Part VIII, with time limits that prevent the procedure from being used to delay access indefinitely. Each regulator should maintain a public register of interoperability requests made to dominant firms and of their outcomes, modelled on the request-tracking arrangements that the European Commission has required of gatekeepers under the Digital Markets Act, so that patterns of refusal become visible.[75] The Cyber Security Authority, for its part, should adopt a practice of reviewing the competitive impact of directives and licensing measures that determine market access, consulting the relevant sectoral regulator before adoption and reviewing such measures at regular intervals.

C. Legislative reforms

Legislation is required to give the test general application beyond the regulated sectors and to secure Ghana's regional and continental obligations. Parliament should enact the long-delayed competition statute, which should prohibit both abuse of dominance and abuse of economic dependence in terms consistent with articles 9 and 11 of the AfCFTA Protocol. The statute should contain an express clause on security justifications, which might be drafted in the following terms.

Conduct by an enterprise in a dominant position, or by an enterprise on which another enterprise is economically dependent, that restricts access to or interoperability with its products, services, interfaces or data shall not be justified on grounds of security, privacy or integrity unless the enterprise establishes that (a) the restriction protects an identified asset against an identified threat by an identified mechanism; (b) that purpose was a reason for the restriction when it was adopted; (c) the restriction materially reduces the threat; (d) the restriction applies equally to the enterprise's own and affiliated services, or any difference in treatment is justified by a distinction relevant to security; and (e) no less restrictive measure would achieve a comparable level of security.

The statute should further require the competition authority to obtain the technical opinion of the Cyber Security Authority before deciding a case under that clause, and should empower it to make orders for access on conditions that preserve security, with powers of suspension and an allocation of liability. Act 1038 should be amended to require the Cyber Security Authority to consider the competitive effects of its directives, standards and licensing measures and to prefer, among measures of comparable security value, those least restrictive of competition. Finally, Parliament should ratify the AfCFTA Protocol on Competition Policy and resolve the status of the ECOWAS competition instruments, so that Ghanaian firms and regulators operate within a coherent regional framework rather than an uncertain one.[76]

XII. CONCLUSION

Security and competition are usually presented as values in tension, with the consequence that every security claim by a dominant firm becomes a reason for competition law to withdraw. This article has argued that the framing is mistaken. Control over what security requires is a form of control over who may compete, and a legal system that accepts security assertions without testing them hands that control to the firms with the strongest incentive to exercise it restrictively. The appropriate response is neither suspicion nor deference but a structured inquiry into whether a security restriction protects an identified asset against an identified threat, whether that purpose existed when the restriction was adopted, whether the restriction works, whether the firm applies it to itself, and whether a less restrictive measure would serve equally well.

The Security Necessity and Symmetry Test provides that inquiry. Its symmetry principle turns the dominant firm's own conduct into evidence of the restriction's purpose; its requirement of contemporaneity distinguishes reasons from rationalizations; its

[75] European Commission, Digital Markets Act developer portal on interoperability, describing the gatekeepers' request processes and Apple's public tracker of interoperability requests submitted since 20 May 2025; Commission Implementing Decision, Case DMA.100204 (n 47).

[76] AfCFTA Protocol (n 25); Legal 500 (n 24).

allocation of burdens follows the Evidence Act 1975 and places the burden of persuasion on the party that holds the relevant knowledge; and its graduated remedies allow pretext to be removed without dismantling protection. Ghana need not await a general competition statute to apply it, since the powers of the National Communications Authority over significant market power, the duty of operators holding such power to share technical information, the Bank of Ghana's demonstrated capacity to mandate secure interoperability and the technical expertise of the Cyber Security Authority are already in place. What has been lacking is a doctrine connecting them. Its adoption would enable Ghana to keep its digital markets open without making them less safe and, as the competition framework of the AfCFTA takes shape, to offer the continent a model for governing security and contestability together.

REFERENCES

1) Case C-233/23 Alphabet Inc and Others v Autorità Garante della Concorrenza e del Mercato (CJEU, 25 February 2025); Court of Justice, press release on the judgment in Case C-233/23 (25 February 2025), recording that Google justified its refusal on security grounds and on the need to allocate the resources required to create a new template.
2) Epic Games Inc v Apple Inc 67 F 4th 946 (9th Cir 2023), cert denied 144 S Ct 682 (2024).
3) Google, announcement of Android developer verification (August 2025), under which verification opened to all developers in March 2026, enforcement began in Brazil, Indonesia, Singapore and Thailand on 30 September 2026 and global expansion is planned from 2027; see also the subsequent introduction of an advanced installation flow for experienced users.
4) LexisNexis, 'Ghana competition and merger control' (Practical Guidance, 2026); CUTS International West Africa, statement on the Consumer Protection and Competition Bills (Accra, 5 December 2025).
5) Electronic Communications Act 2008 (Act 775), s 20, as amended by the Electronic Communications (Amendment) Act 2016 (Act 910); National Communications Authority Act 2008 (Act 769), s 3.
6) National Communications Authority, 'NCA Declares MTN as a Significant Market Power' (Press Release, 9 June 2020); National Communications Authority, 'High Court Dismisses MTN's Case Contesting the NCA's Decision to Declare Them as a SMP in Ghana' (1 September 2020).
7) Ernest Addison, Governor of the Bank of Ghana, speech at the launch of Mobile Money Interoperability Phase II (GhIPSS, Accra, 28 November 2018).
8) Cybersecurity Act 2020 (Act 1038), ss 2 to 4, 35 to 41, 49 to 59 and 92.
9) Joseph Farrell and Paul Klemperer, 'Coordination and Lock-In: Competition with Switching Costs and Network Effects' in Mark Armstrong and Robert Porter (eds), Handbook of Industrial Organization, vol 3 (Elsevier 2007) 1967.
10) Farrell and Klemperer (n 9); see also Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, Competition Policy for the Digital Era (Publications Office of the European Union 2019).
11) Competition and Markets Authority, 'CMA confirms Apple and Google have strategic market status in mobile platforms' (Press Release, 22 October 2025).
12) Auguste Kerckhoffs, 'La cryptographie militaire' (1883) 9 Journal des sciences militaires 5; Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems (3rd edn, Wiley 2020).
13) National Telecommunications and Information Administration, Competition in the Mobile Application Ecosystem (US Department of Commerce, February 2023).
14) NTIA (n 13).
15) Competition and Markets Authority, Mobile Ecosystems Market Study: Final Report (10 June 2022).
16) Citi Business News, report of the statement by the Chief Executive of GhIPSS on the financing of the interoperability platform (May 2018); Citi Business News, report that Phase One was launched on 10 May 2018, connecting the mobile money platforms to the gh-link switch.
17) Addison (n 7); GhIPSS, 'Mobile Money Interoperability ends 2018 with 2.2 million transactions' (January 2019); MyJoyOnline, 'Mobile Money Interoperability records 267% growth in value' (2020), reporting the GhIPSS summary report for 2019.
18) Constitution of the Republic of Ghana 1992, art 36(2).
19) Ghana Lotto Operators Association v National Lottery Authority [2007-2008] SCGLR 1088.
20) Constitution 1992, arts 23 and 296.
21) LexisNexis (n 4).
22) National Petroleum Authority Act 2005 (Act 691); CUTS International West Africa (n 4).
23) Protection Against Unfair Competition Act 2000 (Act 589).
24) Supplementary Act A/SA.1/12/08 adopting Community Competition Rules and the Modalities of their Application within ECOWAS; Supplementary Act A/SA.2/12/08 on the Establishment, Functions and Functioning of the ECOWAS Regional Competition Authority; Legal 500, 'Ghana's Corporate Commercial Outlook 2026' (2026).

25) Protocol to the Agreement Establishing the African Continental Free Trade Area on Competition Policy (adopted 19 February 2023), arts 9 and 11.
26) AfCFTA Protocol (n 25); tralac, 'AfCFTA Protocol on Competition Policy: Factsheet' (October 2023).
27) Act 769, s 3.
28) Act 775, ss 20, 25 and 101 (definition of significant market power).
29) Act 775, s 20. The text of this provision should be read in its form as amended by Act 910.
30) NCA, Press Release (n 6); National Communications Authority, 'Public Information: What SMP Means' (19 June 2023).
31) NCA, 'High Court Dismisses MTN's Case' (n 6).
32) Act 775, ss 88 to 92.
33) Payment Systems and Services Act 2019 (Act 987), ss 3 and 7(2)(f).
34) Act 987, s 101; Bank of Ghana, Guidelines for Domestic Processing of Payment Card Transactions, issued under s 101(2).
35) Bank of Ghana, Cyber and Information Security Directive (2018).
36) Act 1038 (n 8).
37) Ghana News Agency, 'CSA fines ORC GH₵240,000 over cybersecurity non-compliance' (13 August 2026).
38) Data Protection Act 2012 (Act 843), s 28.
39) Case C-7/97 Oscar Bronner GmbH & Co KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co KG [1998] ECR I-7791.
40) Case C-418/01 IMS Health GmbH & Co OHG v NDC Health GmbH & Co KG [2004] ECR I-5039.
41) Case T-201/04 Microsoft Corp v Commission [2007] ECR II-3601.
42) Alphabet v AGCM (n 1).
43) ibid.
44) Case C-738/22 P Google LLC and Alphabet Inc v Commission (CJEU, 2 July 2026), dismissing the appeal against Case T-604/18 Google and Alphabet v Commission (Google Android) (General Court, 14 September 2022).
45) 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) [2022] OJ L265/1, art 6(7) and recital 50.
46) DMA (n 45), arts 6(4) and 7.
47) Commission Implementing Decision of 19 March 2025, Case DMA.100203, Article 6(7), Apple, iOS, Features for Connected Physical Devices, C(2025) 3000, summary at OJ C/2025/4646; Commission Implementing Decision of 19 March 2025, Case DMA.100204 (process for interoperability requests).
48) United States v Microsoft Corp 253 F 3d 34 (DC Cir 2001) (en banc).
49) Aspen Skiing Co v Aspen Highlands Skiing Corp 472 US 585 (1985); Verizon Communications Inc v Law Offices of Curtis V Trinko LLP 540 US 398 (2004).
50) Epic Games v Apple (n 2).
51) ibid; see the questions presented in Epic's petition for certiorari, Epic Games Inc v Apple Inc, No 23-337 (filed 27 September 2023), concerning the test for a less restrictive alternative.
52) United States v Apple Inc, No 2:24-cv-04055 (D NJ, 30 June 2025) (order denying motion to dismiss).
53) Digital Markets, Competition and Consumers Act 2024.
54) CMA (n 11); Competition and Markets Authority, 'The CMA's programme of work across mobile platforms' (guidance, updated 2026).
55) Competition Act 89 of 1998 (South Africa), s 8.
56) Competition Act 2010 (Kenya), s 24; Federal Competition and Consumer Protection Act 2018 (Nigeria), ss 70 to 72.
57) See the announcement cited at (n 3) and the public objections of the F-Droid project and the Keep Android Open campaign (2025 and 2026).
58) United States v Apple (n 52).
59) Act 1038, ss 49 to 59; Ghana News Agency (n 37).
60) Microsoft v Commission (n 41).
61) Epic Games v Apple (n 2).
62) Evidence Act 1975 (NRCD 323), ss 10 and 11.
63) NRCD 323, s 14.
64) NRCD 323, s 12.
65) R v Turner (1816) 5 M & S 206, 105 ER 1026.
66) On confidentiality rings, see the Competition Appeal Tribunal Rules 2015 (SI 2015/1648) and the practice of the Competition Appeal Tribunal; on data rooms, European Commission, Best Practices on the disclosure of information in data rooms in proceedings under Articles 101 and 102 TFEU and under the EU Merger Regulation (2015).

67) Act 1038, ss 3, 4 and 35 to 41.
68) High Court (Civil Procedure) Rules 2004 (CI 47), Order 55; Constitution 1992 (n 20).
69) Microsoft v Commission (n 41), annulling art 7 of the Commission's decision.
70) Act 769, s 3; Act 987 (n 33) and s 101; Act 1038, ss 3 and 4.
71) Trinko (n 49).
72) See Part II.C above and the sources cited at (n 17).
73) Crémer, de Montjoye and Schweitzer (n 9); Stigler Committee on Digital Platforms, Final Report (George J Stigler Center for the Study of the Economy and the State, University of Chicago Booth School of Business 2019); Herbert Hovenkamp, 'Antitrust and Platform Monopoly' (2021) 130 Yale LJ 1952; Lina M Khan, 'Amazon's Antitrust Paradox' (2017) 126 Yale LJ 710.
74) DMA (n 45), art 6(7).
75) European Commission, Digital Markets Act developer portal on interoperability, describing the gatekeepers' request processes and Apple's public tracker of interoperability requests submitted since 20 May 2025; Commission Implementing Decision, Case DMA.100204 (n 47).
76) AfCFTA Protocol (n 25); Legal 500 (n 24).