The DMA Compliance Trap:

How the EU Is Regulating AI Into Insecurity

Dr. Diana Năsulea

Programmes Manager and Researcher at IES Europe

Dr. Christian Năsulea

Executive Director at IES Europe

9 April 2026

Summary

- On 27 January 2026, the European Commission launched two specification proceedings against Google under the Digital Markets Act (DMA), requiring it to open Android's artificial intelligence (AI) system features to rival services and share search data with competitors. These are the first DMA proceedings targeting artificial intelligence directly, and the precedent they set will shape platform regulation across Europe and beyond.

- The briefing argues that the Commission's current approach creates three unresolved contradictions. First, the requirement to open Android's deepest system features to third-party AI services conflicts directly with the EU's Cyber Resilience Act (CRA), which mandates minimum necessary access as a security principle. Second, the obligation to share search data at scale conflicts with the General Data Protection Regulation's (GDPR) anonymisation standards. Third, the specification is calibrated to today's conversational AI assistants but contains no mechanism to revise access rights as AI evolves toward autonomous agents capable of acting without continuous user oversight.

- The briefing also examines the geopolitical dimension. The proceedings have been launched into an already hostile transatlantic environment, with the US administration characterising EU digital regulation as discriminatory and proposing significant trade retaliation. The specification decisions adopted in 2026 will either give those critics evidence for their case or undercut it.

- As a solution, the briefing proposes a tiered access framework: open app-level access for all, deep system access conditioned on CRA certification, and search data access conditioned on GDPR-compliant privacy safeguards. This approach would achieve the DMA's pro-competitive objectives while maintaining coherence with the EU's own security and privacy standards, and offer a more credible model for adoption by other jurisdictions following the Brussels model.

- Alongside the Tiered Access Framework, the briefing argues that user choice should be restored to the centre of the access question. A framework in which third-party AI services can request system-level access, and users can grant or deny it on an informed and reversible basis, would achieve the DMA's contestability objective without overriding the individual autonomy that the EU's data protection framework is built to protect. Competition policy should facilitate user choice, not substitute for it.

Table of contents

SUMMARY 1

TABLE OF CONTENTS 2

INTRODUCTION 4

WHAT THE COMMISSION IS DECIDING – AND WHY THE PRECEDENT IS DANGEROUS 5

OPEN IT UP VS. KEEP IT SECURE: THE DMA–CRA COLLISION 7

SHARE THE DATA VS. PROTECT PRIVACY: THE DMA–GDPR COLLISION 9

LEVEL THE PLAYING FIELD VS. HAND OVER THE KEYS: THE AUTONOMOUS AGENT PROBLEM 10

THE TRANSATLANTIC DIMENSION: REGULATION AS A TRADE WEAPON 13

THE SOLUTION: A TIERED-ACCESS FRAMEWORK 14

POLICY RECOMMENDATIONS 16

CONCLUSION 17

REFERENCES 18

About the authors

Dr. Diana Năsulea holds a PhD in Economics and serves as Programmes Manager and Researcher at IES-Europe (Institute for Economic Studies – Europe), where she designs and coordinates educational programs, international seminars, and policy research projects promoting classical liberal ideas and economic freedom across Europe. Her research focuses on EU digital and trade policy, exploring their effects on competitiveness, SMEs, and national economies. She has authored numerous research and academic papers in these areas. Beyond her work with IES-Europe, Diana is a Teaching Associate at the University of Bucharest's Faculty of History.

Dr. Christian Năsulea teaches Economics at the Department of International Relations and Universal History at the Faculty of History of the University of Bucharest. He is the Executive Director of the Institute for Economic Studies – Europe and a fellow of the Institute for Research in Economic and Fiscal Issues. His areas of research interest include public policy and stimuli for economic development, political and commercial negotiation in international relations, behavioural economics and decision processes. In addition to his university work he is also a tech entrepreneur, developing software and hardware solutions, but also learning resources for high school students who are interested in economics.

About EPICENTER

EPICENTER, the European Policy Information Center, is an independent initiative of twelve leading think tanks from across Europe. It seeks to inform the European policy debate and promote the principles of a free society by bringing together the expertise of its members.

EPICENTER is formed by the Center for Political Studies (Denmark), Civil Development Forum (Poland), Fundalib (Spain), the Institut economique Molinari (France), the Institute of Economic Affairs (UK), the Institute of Economic and Social Studies (Slovakia), the Institute for Market Studies (Bulgaria), Istituto Bruno Leoni (Italy), KEFiM (Greece), the Lithuanian Free Market Institute, Prometheus (Germany), and Timbro (Sweden). Like its members, EPICENTER is politically independent and does not accept taxpayer funding.

Introduction

On 27 January 2026, the European Commission launched two specification proceedings against Google[1] under the Digital Markets Act (DMA), targeting artificial intelligence (AI) interoperability on Android (Article 6(7)) and the sharing of search data with third parties (Article 6(11)). These proceedings go far beyond previous DMA enforcement actions. For the first time, the Commission is attempting to mandate deep, system-level access to platforms and data for AI systems that are inherently unpredictable and whose capabilities are evolving rapidly. The precedent set here will define how AI platforms are regulated in Europe, and increasingly, globally.

The current approach raises a series of structural challenges. By extending interoperability obligations to core system functions and large-scale data access, the proceedings introduce tensions that existing regulatory frameworks are not designed to resolve. Unlike earlier cases involving well-defined technical protocols, these proceedings concern technologies whose behaviour cannot be fully specified in advance and whose capabilities are more dynamic than regulatory cycles.

At the core of the issue are unresolved contradictions between key elements of the EU's digital regulatory framework. The DMA's requirement for broad interoperability is in tension with the Cyber Resilience Act's (CRA) 'secure by design' principle, which emphasises limiting access to what is strictly necessary. Similarly, the obligation to share search data under Art. 6(11) intersects with the General Data Protection Regulation's (GDPR) stringent requirements related to anonymisation, data minimisation, and purpose limitation. Expanding access to sensitive system features and behavioural data increases the complexity of maintaining these protections and raises questions about how they can be enforced consistently across different actors.

These challenges are complicated further by the characteristics of AI systems. As capabilities expand from assistive functions to increasingly autonomous behaviour, the implications of system-level access change significantly. Permissions that are calibrated to current use cases may become inadequate as AI systems gain the ability to initiate actions, interact across services, and operate with reduced human oversight. At the same time, the DMA's specification process does not include mechanisms for automatic adaptation to such technological shifts.

Implementation constraints add another layer of complexity. Android operates within a highly fragmented ecosystem of thousands of device models and independent manufacturers, making the uniform application of detailed technical requirements difficult in practice. In parallel, the increased scope of obligations creates asymmetries across the competitive landscape and may influence how and where new functionalities are developed and deployed.

Moreover, these proceedings are also unfolding within a broader international context in which digital regulation is increasingly linked to trade and geopolitical considerations. The standards established through these decisions are likely to extend beyond the EU, shaping regulatory approaches in other jurisdictions.

To address these challenges, this briefing proposes a 'tiered-access framework' that aligns interoperability obligations with the sensitivity of the access granted. Basic application-level access would remain available broadly, while deeper system access and access to behavioural data would be conditional on compliance with cybersecurity certification and data protection requirements. This approach introduces a proportional structure that supports interoperability while maintaining coherence with existing legal frameworks.

The Commission's decisions in these proceedings will play a defining role in shaping the governance of AI-enabled platforms. Ensuring that these decisions are internally consistent, adaptable, and aligned with the broader regulatory environment will be critical for their long-term effectiveness.

1. What the commission is deciding – and why the precedent is dangerous

On 27 January 2026, the European Commission opened two concurrent specification proceedings against Google under the Digital Markets Act — the first time the DMA's interoperability obligations have been directed explicitly at artificial intelligence. Unlike previous enforcement actions, which addressed well-defined platform behaviours in established markets, these proceedings concern technologies whose capabilities are evolving faster than any regulatory specification can anticipate. Understanding what the Commission is deciding, and why the structural features of these proceedings make the precedent unusually consequential, is the necessary starting point for evaluating the framework proposed in this briefing.

1.1. The proceedings

The two specification proceedings formalise the Commission's ongoing regulatory dialogue with Google. By April 2026, the Commission will issue preliminary findings setting out draft measures; by July 2026, a final specification must be adopted. Non-compliance will trigger fines of up to 10% of global annual turnover, and up to 20% for repeat infringements.

The first proceeding targets Android features that only Gemini can currently access: neural processing units (NPUs) for on-device AI inference; system-level microphone and voice-trigger application programming interfaces (APIs); always-on listening capabilities; screen-reading permissions; and sensor access. The Commission intends to specify how Google must grant 'equally effective' access to these same features to third-party AI services.

The second proceeding targets Google's obligation under Art. 6(11) to share search signals – such as rankings, queries, clicks, and views data – with rivals on FRAND[2] terms. Unusually, it also examines whether AI chatbot providers qualify as eligible recipients, acknowledging that the boundary between 'search' and 'conversational AI' has dissolved.

> Commission (27 Jan 2026):[3] 'The Commission intends to specify how Google should grant third-party AI service providers equally effective access to the same features as those available to Google's own services'.

---

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

[2] Fair, reasonable, and non-discriminatory (FRAND): Principle requiring holders of essential technologies or gatekeepers to grant access under fair and proportionate conditions, with comparable terms for similar users, in order to prevent abuse of market power while preserving incentives for innovation.

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

1.2. Why are these proceedings structurally different from previous DMA actions?

Prior DMA interoperability mandates addressed deterministic, well-established protocols, such as messaging bridges, NFC, Bluetooth, and app store connectivity. Technical parameters were bounded, access rights were specifiable in advance, and compliance could be verified against a fixed standard. These proceedings are different in three ways that matter enormously for the precedent they set.

- **Non-determinism:** AI systems with microphone access, screen-reading permissions, and NPU access do not behave according to a fixed standard. The same permissions that enable a legitimate calendar assistant can also allow access to private messages, financial credentials, or the initiation of transactions by the assistant itself or by malicious actors exploiting the same access. Unlike Bluetooth, AI outcomes cannot be fully specified in advance.
- **Capability evolution:** AI capabilities advance faster than any regulatory specification cycle. A specification calibrated to today's assistants will be applied to tomorrow's autonomous agents, which may be capable of planning multi-step tasks, initiating payments, and controlling device functions without continuous human oversight.
- **Fragmented implementation:** Android runs on more than 24,000 device models produced by hundreds of original equipment manufacturers (OEMs). Meaningful compliance requires coordination with chip manufacturers, device makers, and software developers entirely outside Google's contractual reach.

The precedent effect extends far beyond Google. Every subsequent AI interoperability proceeding against Apple, Microsoft, or any future designated platform will be judged against what the Commission decides here. The EU is writing the global rulebook for AI platform access in six months, in the middle of a transatlantic trade war, without a mandatory security review.

1.3. The DMA was not built for this

A growing body of work in legal scholarship and competition economics is questioning whether the DMA is structurally suited to regulate AI at all; these concerns are directly relevant to what the Commission is now attempting to specify.

Bostoen and Krämer (2025) identify a foundational tension: the DMA was designed for platforms, not technologies. AI is a general-purpose technology that cuts across multiple platform categories simultaneously. Applying Art. 6(7) interoperability obligations to AI-system features across the Android operating system (OS) is an indirect approach to a structural problem, and one that creates significant compliance complexity without necessarily addressing the underlying competition dynamics.

Additionally, a concern that must be addressed regarding AI is that DMA obligations are specified after AI models are already built. By the time a specification decision is adopted and implemented, the training data has already been collected, the models developed, and the architecture fixed. Compliance mandates that arrive after the fact cannot undo competitive dynamics established during the development phase – they can only affect the deployment layer (Ribera Martínez 2024).

There is also growing concern about the asymmetry in the DMA's AI enforcement logic (Ribera Martínez 2024). By design, the DMA applies only to designated gatekeepers. Some of the biggest AI companies with large language models (LLMs) used by hundreds of millions of people face no DMA obligations because they do not operate a designated core platform service. The specification proceedings target Google's AI and its access to the Android OS, while leaving other AI companies' competitive position entirely unaddressed. The regulation mandates openness from incumbents while leaving the most disruptive challengers outside its scope altogether.

2. Open it up vs. keep it secure: The DMA–CRA collision

The specification proceedings do not occur in a regulatory vacuum. They sit alongside two other major EU frameworks — the Cyber Resilience Act and the GDPR — each pursuing legitimate but competing objectives. Where the DMA mandates openness, the CRA mandates restraint, and the GDPR mandates minimisation. Applied simultaneously to the same system-level features and the same datasets, these frameworks produce obligations that cannot all be satisfied at once. The Commission has not acknowledged this conflict, let alone resolved it.

2.1. A self-contradictory regulatory landscape

The Commission is simultaneously enforcing two EU frameworks whose core requirements point in opposite directions. The DMA's Art. 6(7) mandates maximum openness: third-party AI services must receive Android access equivalent to that of Gemini. On the other hand, the CRA's 'secure by design' mandate demands minimum necessary access – the 'principle of least privilege', requiring that platforms provide third parties only the minimum necessary access to functioning (Official Journal of the European Union 2024). These two requirements are structurally irreconcilable when applied to the same system-level features.

On the one hand, a gatekeeper that opens up NPU access, microphone APIs, and screen-reading permissions to all qualifying third parties is, by the CRA's own logic, creating attack surfaces that did not previously exist. On the other, a gatekeeper that restricts permissions to what is strictly necessary may be found in violation of the DMA's 'equally effective' standard. The Commission has provided no resolution mechanism for this conflict. The Center for Strategic and International Studies (CSIS) observes that every DMA compliance solution achieved to date has produced 'unforeseen consequences in reduced efficiency and consumer protection'.[4] And it was referring to solutions for relatively simple platform rules, not deep AI system access.

2.2. The concrete security risks

The regulatory conflict identified above is not merely theoretical. Mandating deep system-level access for third-party AI services creates concrete and measurable security risks that existing mobile security architectures were specifically designed to prevent. Four categories of risk are particularly relevant to the Commission's current specification proceedings.

2.2.1. Expanded attack surfaces

Modern mobile operating systems were deliberately designed to avoid the persistent vulnerabilities of traditional desktop computing. The layered, tiered security architecture of Apple's OS (iOS) and Android exists precisely to limit the blast radius of any single compromise. The CrowdStrike incident of 2024[5] demonstrated that kernel-level access,[6] even by a legitimate, vetted provider, can cause cascading global system failures when a single update goes wrong. Art. 6(7) would extend similarly

---

[4] 'Guarding the gates: The Digital Markets Act and lessons in ex ante regulation', Center for Strategic and International Studies, 5 January 2026 (https://www.csis.org/blogs/charting-geoeconomics/guarding-gates-digital-markets-act-and-lessons-ex-ante-regulation).

[5] 'What the 2024 CrowdStrike glitch can teach us about cyber risk', Harvard Business Review, 10 January 2025 (https://hbr.org/2025/01/what-the-2024-crowdstrike-glitch-can-teach-us-about-cyber-risk).

[6] Kernel-level access: The highest level of system access in an operating system, allowing software to interact directly with core system functions (memory, hardware, and processes) with full privileges, rather than being restricted similarly to normal applications.

deep access to any qualifying third-party AI service provider, including those with far weaker security practices than CrowdStrike.

The International Center for Law & Economics (ICLE) documents, in the context of Apple's parallel iOS compliance proceedings, that third parties have already invoked Art. 6(7) to request access to Apple's Just-In-Time Compiler engine. If granted, it would represent a 'major security vulnerability' according to the cybersecurity community, as it allows arbitrary code execution at the core OS level.[7] These requests illustrate the type of demands the Commission is likely to face under the current Android specification proceedings.

2.2.2. Overbroad access requests and data harvesting

In a review, the Center for European Policy Analysis' (CEPA)[8] finds that developers are already requesting access to notification content, Wi-Fi history, and full message histories. The ICLE has received third-party requests for the ability to 'read the contents from each and every message and email on the user's device'. Apple has publicly stated that cybersecurity agencies were 'nowhere to be found' in discussions in key DMA interoperability decisions, leaving these requests without independent security scrutiny (Centre for Information Policy Leadership 2024).

These conditions recreate the environment that enabled Cambridge Analytica scandal – open API access, inadequate controls on request scope, and no effective mechanism to prevent data collected for one stated purpose from being used for another.

2.2.3. The free-rider problem and innovation withdrawal

The DMA's interoperability mandate not just opens access but also eliminates, or at least reduces, the competitive advantage that platforms have built through investment. The ICLE[9] identifies what it calls the 'Harrison Bergeron' dynamic: 'openness', 'neutralisation', and 'design transparency' are treated as proxies for regulatory success even when they undermine scale and scope economies, degrade security through weaker default protections, or substitute one set of frictions for another.

Innovation withdrawal has already been documented as a tangible consequence of the DMA. Apple initially withheld its Apple Intelligence suite from EU users for approximately six months, citing compliance risks.[10] The company has since delayed or withheld additional features from European consumers, including live translation for AirPods, iPhone mirroring (phone mirroring), and enhanced SharePlay screen sharing. These restrictions stem from DMA interoperability obligations that require platforms to open up low-level system controls that currently safeguard user privacy and security.

---

[7] 'Response to first review of the Digital Markets Act', Manne, Radic & Auer, International Center for Law & Economics, September 2025; 'Comparing the EU DMA to the search-query data-sharing remedy in US v. Google', International Center for Law & Economics, 24 September 2025 (https://laweconcenter.org/resources/icle-response-to-first-review-of-the-digital-markets-act/).

[8] 'Europe's DMA — A cybercriminal's paradise?', Center for European Policy Analysis, January 2026; 'Opening up — Europe's DMA and the risks of interoperability', Center for European Policy Analysis, 13 November 2025 (https://cepa.org/article/europes-dma-a-cybercriminals-paradise/).

[9] 'EU DMA workshops: Google, Amazon, Apple, Meta, and Microsoft', EUTechReg, 8 July 2025 (https://eutechreg.com/p/eu-dma-workshops-google-amazon-apple).

[10] 'Apple to delay launch of AI-powered features in Europe, blames EU tech rules', Reuters, 21 June 2024 (https://www.reuters.com/technology/artificial-intelligence/apple-delay-launch-ai-powered-features-europe-blames-eu-tech-rules-2024-06-21/).

Google has similarly highlighted that the 'withholding of innovations from Europe'[11] is a direct outcome of regulatory pressure to comply with the DMA. As obligations extend further to AI, this pattern is expected to intensify. Ribera Martínez (2024) warns that providers may ultimately 'limit the features they will roll out in the EU altogether', resulting in European consumers being denied access to, and the ability to interact with, functionalities specifically tailored to their needs.

2.2.4. The non-EU competitive asymmetry

An additional concern relates to the asymmetric regulatory burden imposed by the DMA on firms operating within its jurisdiction. Major non-EU digital ecosystems, including those developed by Chinese companies such as Huawei, Tencent, Xiaomi, and Baidu, are not subject to equivalent interoperability or data-sharing obligations. These firms retain the ability to operate vertically integrated and tightly controlled system architectures, which may offer advantages in terms of security, performance, and product integration.

At the same time, alternative app distribution channels are already present on Android devices within the EU, suggesting that competitive dynamics are not confined to DMA-designated gatekeepers alone. The current specification proceedings risk reinforcing this asymmetry by requiring EU and US-based platforms to provide open access to sensitive system functionalities, while competitors operating outside the DMA's scope are not subject to comparable constraints.

Policy analysis has increasingly highlighted that unilateral regulatory approaches in digital markets may generate unintended competitive distortions when not aligned with other major jurisdictions. For instance, the CSIS[12] highlights that divergences in regulatory frameworks can influence relative competitiveness and innovation incentives across global markets. In this context, the ongoing specification proceedings may deepen, rather than mitigate, existing asymmetries in the global digital ecosystem.

3. Share the data vs. protect privacy: The DMA–GDPR collision

The collision between the DMA and the EU's cybersecurity framework is not the only internal contradiction these proceedings expose. The obligation to share search data under Article 6(11) creates an equally fundamental tension with the GDPR — one that goes to the mathematical relationship between privacy protection and competitive utility, and that the Commission has yet to resolve before requiring compliance with both simultaneously.

3.1. The inescapable tension in Article 6(11)

Search query data is not a neutral commercial record. It often contains information on health concerns, financial circumstances, political orientation, and daily behaviour across hundreds of millions of users. Even stripped of direct identifiers, sequential query data can enable the reconstruction of individual profiles through pattern analysis and inference – these are precisely the re-identification vectors the GDPR requires anonymisation to neutralise.

---

[11] 'Google warns EU against 'erecting walls' in tech sovereignty push`, Financial Times, 13 February 2026 (https://www.ft.com/content/0847914c-be27-4573-8600-8cdb54e604b7?syn-25a6b1a6=1)

[12] 'Guarding the gates: The Digital Markets Act and lessons in ex ante regulation', Center for Strategic and International Studies, 5 January 2026 (https://www.csis.org/blogs/charting-geoeconomics/guarding-gates-digital-markets-act-and-lessons-ex-ante-regulation).

The DMA's Recital 61 instructs gatekeepers to share this data while protecting users against re-identification risks 'without substantially degrading the quality or usefulness of the data'.[13] This instruction is self-defeating. Anonymisation rigorous enough to satisfy the GDPR's re-identification threshold necessarily destroys the competitive utility the DMA is trying to unlock.

No binding implementing act has been adopted specifying which anonymisation standard satisfies both frameworks simultaneously. No shared privacy baseline governs what recipients may do with the data once received. Google, therefore, faces GDPR enforcement if it shares too much and DMA non-compliance proceedings if it shares too little. That is not a compliance framework but rather a liability trap, and the Commission has opened specification proceedings without resolving it.

3.2. The utility–privacy paradox

The GDPR's anonymisation standard requires that data be rendered irreversibly non-identifiable to mitigate three re-identification risks: singling out, linkability, and inference. Achieving that standard for search query data requires aggressive thresholding and suppression. Evidence cited in the US v. Google federal remedy proceedings confirms that Google's own proposed anonymisation solution excluded approximately 99% of queries from the shared dataset.[14] GDPR-compliant datasets include the most common queries, precisely those that rivals can already access through public signals, not the long-tail queries that differentiate a high-quality search engine.

3.3. Downstream privacy risks: The problem of the weaker recipient

The DMA's data-sharing mandate creates a privacy risk rarely discussed: the recipients of shared search data typically have weaker data governance, security infrastructure, and compliance resources than the gatekeeper from which the data is taken (Centre for Information Policy Leadership 2024). The European Data Protection Board (EDPB)–Commission draft joint guidelines acknowledge this risk, proposing implementing acts that will allow gatekeepers to impose contractual conditions on recipients. However, as of April 2026, no such implementing act has been adopted. The Commission is opening proceedings that will require data sharing at scale before the safeguards that would make that sharing safe have been defined.

There is also a purpose limitation problem that the guidelines do not adequately address. Search data shared under Art. 6(11) to improve search ranking may not be lawfully reused by recipients to train AI models, build user profiles, or serve advertising. But enforcing purpose limitations across dozens of recipients in multiple jurisdictions is a contractual exercise, not a technical one. Additionally, contractual constraints on data use, without technical enforcement, are notoriously difficult to uphold at scale.

4. Level the playing field vs. hand over the keys: The autonomous agent problem

The tensions identified in the preceding sections concern conflicts between existing legal frameworks. The challenge examined here is different in kind: the specification proceedings are

---

[13] `Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation`, European Commisin & European Data Protection Baord, n.d. (https://digital-markets-act.ec.europa.eu/document/download/8ba0913f-2778-4a6d-9c58-10f8c7ead009_en?filename=Joint_COM-EDPB_GLS_interplay_DMA_GDPR_for_public_consultation.pdf)

[14] United States District Court for the District of Columbia, Case No. 20-cv-3010 (APM) (https://deadline.com/wp-content/uploads/2025/09/gov.uscourts.dcd_.223205.1436.0_4.pdf).

being drafted for an AI landscape that is already changing beneath them. Even if the DMA-CRA and DMA-GDPR conflicts were fully resolved, the Commission would still face the problem of writing rules for a technology whose most consequential capabilities, namely autonomous action, independent decision-making, and operation without human oversight, lie just ahead, not in the past the DMA was designed to address.

4.1. The DMA was designed for yesterday's problems

The specification proceedings are being drafted in the context of the early-2026 AI landscape, in which the relevant services are conversational assistants – systems that answer questions, read calendars, and set reminders. The access rights the Commission is defining are calibrated to these use cases. The problem is that technologies will not stop here.

The DMA's core structural limitation is that it 'was adopted to address known competition issues in digital markets, in other words, problems of the past' (Bostoen and Krämer, 2025), and its 'effectiveness with regard to emerging technologies' is therefore 'an open question'. The DMA does provide some protection against near-term risks of AI systems being excluded from platforms through its existing OS interoperability obligations, but this effect is incidental rather than intentional. The obligations Art. 6(7) imposes were developed to address app store access and connected device interoperability, not to govern autonomous systems capable of initiating financial transactions, accessing personal communications, and executing multi-step tasks without continuous user oversight.

Nonetheless, a short-term workaround exists. Agentic AI could plausibly be designated under the existing 'virtual assistant' core platform service category without requiring full legislative amendment.[15] But this does not resolve the specification decision's underlying problem. That category was designed with voice-activated assistants in mind – namely, systems equipped for information retrieval and device control within defined parameters. Applying it to autonomous agents operating across email, payments, calendars, and external APIs, with non-deterministic outputs and prompt-injection vulnerabilities, stretches the category well beyond its design intent. Access rights appropriate for a voice assistant in 2023 are not the right template for an autonomous agent in 2026.

The Commission is therefore in a position where the specification decision it adopts in July 2026 will govern AI access rights on the world's dominant mobile OS for the foreseeable future, without a built-in mechanism to revise those rights as the technology changes and against a standard of 'equally effective access' that was never written with agentic AI behaviour in mind.

4.2. The agentic security gap

Autonomous AI agents are moving rapidly into enterprise production. Industry data from early 2026 shows that 80.9% of enterprise technical teams have moved past the pilot stage to active testing or production. Only 14.4% of organisations reported agentic AI going live with full security and IT

[15] 'EDPB and European Commission issue joint guidelines on intersection of DMA and GDPR', Mondaq, 12 November 2025 (https://www.mondaq.com/unitedstates/privacy-protection/1703848/edpb-and-european-commission-issue-joint-guidelines-on-intersection-of-dma-and-gdpr).

approval.[16] Around 80% reported risky agent behaviours, including unauthorised system access and improper data exposure.[17]

For a conversational assistant, system-level access enables better context awareness, which is useful but bounded. For an autonomous agent with the same access rights, the risk is categorically different. An agent with full device access – microphone, screen, NPU, sensors, email, calendar, contacts, payment credentials – and the ability to act autonomously is, in practical terms, a system with total control over a user's digital life. The specific attack vector that makes this dangerous is prompt injection: malicious instructions embedded in content that the agent reads, which cause it to take unintended actions. The Open Worldwide Application Security Project (OWASP)[18] ranked prompt injection as the top LLM vulnerability in 2025. The National Institute of Standards and Technology's (NIST) January 2026 AI Agent Standards[19] Initiative was launched because existing security frameworks do not address this threat at the agentic level.

4.3. Static specifications cannot govern dynamic technology

Once adopted, specification decisions remain in effect until a new proceeding replaces them. The DMA's enforcement framework contains no automatic mechanism to revise a specification decision when the technology it governs undergoes a qualitative shift, as AI capabilities that evolve rapidly over months. Access rights defined for voice assistants in 2026 will be available to autonomous agents in 2027 and 2028. The Commission has proposed no mechanism to address this. The question – how future-proof the DMA is – therefore deserves a formal answer before the specification decision is finalised.

4.4. User choice and interoperability

Another dimension that the specification proceedings do not address is user choice. The Commission treats the access question as a matter to be resolved between the regulator and the gatekeeper. Once the specification is adopted, qualifying third-party AI services will receive equivalent system-level access as a regulatory right. The user whose device is being accessed and whose data flows through the mandated access point is not a party to that determination.

This is not a trivial omission. The GDPR's consent architecture rests on the principle that individuals should exercise meaningful control over how their personal data is accessed and by whom. A user who actively chooses to grant a rival AI assistant the same microphone and screen permissions as Gemini is making an informed decision about their own device and data – something that competition policy should facilitate, not pre-empt. A user who does not make that choice should not find that the choice has been made for them by a specification decision they had no role in shaping.

The Commission's own compliance workshops have revealed the problem with removing user preference from the equation. The Commission treats low adoption rates for mandated

---

[16] 'State of AI agent security 2026 report: When adoption outpaces control', Gravitee, 4 February 2026 (https://www.gravitee.io/blog/state-of-ai-agent-security-2026-report-when-adoption-outpaces-control).

[17] 'AI went from assistant to autonomous actor — and security never caught up', Help Net Security, 3 March 2026 (https://www.helpnetsecurity.com/2026/03/03/enterprise-ai-agent-security-2026/).

[18] 'LLM01: Prompt Injection', OWASP GenAI Security Project, 2025 (https://genai.owasp.org/llmrisk/llm01-prompt-injection/).

[19] 'Request for information regarding security considerations for artificial intelligence agents', NIST, 8 January 2026 (https://www.nist.gov/news-events/news/2026/01/caisi-issues-request-information-about-securing-ai-agent-systems).

interoperability features as evidence of non-compliance rather than as evidence that users, when given a genuine choice, preferred the service as originally designed.[20] A user-controlled permission framework, in which third-party AI services can request system-level access, and users can either grant or deny it on an informed and reversible basis, would achieve the DMA's contestability objective without overriding the individual autonomy that the EU's data protection framework is built to protect. It would also substantially reduce the security risks identified in Section 2, as access granted by an informed user to a specific service they have chosen is a categorically different risk profile from access mandated uniformly across all qualifying applicants.

5. The transatlantic dimension: Regulation as a trade weapon

The regulatory contradictions examined in the preceding sections are primarily legal and technical in nature. The challenge examined here operates at a different level entirely. The specification proceedings against Google have been launched into a transatlantic relationship under acute strain, in which EU digital regulation has become a direct object of US trade policy. The Commission's decisions in July 2026 will be read not only as competition enforcement but as a geopolitical signal — and the stakes of getting that signal wrong extend well beyond the digital sector.

5.1. The geopolitical context

The specification proceedings against Google were launched in the most hostile transatlantic digital policy environment in decades. The Trump administration has characterised EU digital regulation as 'designed to harm, or discriminate against, American Technology'.[21] Section 301 investigations into EU digital rules have been initiated. Tariff packages of up to $200 billion targeting European goods have been proposed in direct response to DMA enforcement.[22] US Commerce Secretary Howard Lutnick reportedly proposed that the EU roll back tech regulations in exchange for a steel and aluminium deal. The US State Department imposed visa restrictions on five EU officials involved in drafting the DMA and DSA.[23] In this complex geopolitical environment, digital regulations that primarily target American companies should proceed with caution in order to avoid decisions that seem discretionary or retaliatory.

> **US House Judiciary Committee:**[24] The DMA does not ask whether consumers have been harmed. It does not even ask whether a business has done anything wrong. It asks whether a company is large, successful, and, most importantly, American. If the answer is yes, the rules suddenly change. — *Rep. Scott Fitzgerald (R-WI), December 2025*

---

[20] 'EU DMA workshops: Google, Amazon, Apple, Meta, and Microsoft', EUTechReg, 8 July 2025 (https://eutechreg.com/p/eu-dma-workshops-google-amazon-apple).

[21] 'The EU's Digital Markets Act and Digital Services Act: An explainer for transatlantic policy', German Marshall Fund of the United States, 15 October 2025 (https://www.gmfus.org/news/eus-digital-markets-act-and-digital-services-act).

[22] 'EU prepares tougher tech enforcement in 2026 as Trump warns of retaliation', European Business Magazine, 6 January 2026 (https://europeanbusinessmagazine.com/european-news/eu-prepares-tougher-tech-enforcement-in-2026-as-trump-warns-of-retaliation/).

[23] 'The new containment doctrine: How the United States is using trade to stop digital regulation', Center for Strategic and International Studies, 9 March 2026 (https://www.csis.org/analysis/new-containment-doctrine-how-united-states-using-trade-stop-digital-regulation).

[24] 'Post on DMA / digital policy', Policy Solution, X (formerly Twitter), March 2026 (https://x.com/Policy_Solution/status/2000952000565961109).

5.2 The cost of regulating unilaterally

The CSIS[25] identifies the DMA's drafting history as a strategic error whose consequences are now clearly visible: 'By crafting the DMA without U.S. partnership, the EU opened itself up to backlash when five of the seven identified gatekeepers were American. Every solution to non-compliance has led to unforeseen consequences in reduced efficiency and consumer protection, all while doing little to win back the United States' favour'.

The US administration has moved beyond bilateral pressure on the EU, embedding anti-digital regulation clauses into trade agreements with partners across Southeast Asia and Latin America. It is also attempting to leverage tariffs to contain the spread of DMA-like frameworks before they take root.[26] The specification decisions adopted in July 2026 will determine whether the US containment strategy has an easy case to make or a hard one: a specification that mandates system-level AI access without security preconditions hands Washington precisely the evidence it needs to characterise EU digital regulation as protectionism; a proportionate, safeguards-conditioned framework substantially undercuts that argument.

5.3 The Brussels effect: Exporting a flawed standard

The impact of the DMA's specification decisions will not be limited to Europe. Japan, Brazil, India, and Australia have all adopted or are considering DMA-like frameworks. If the July 2026 specification mandates system-level AI access without security preconditions, the EU will have exported a security-degrading standard to every jurisdiction that follows its lead, while Chinese platforms in every one of those jurisdictions will remain unaffected. A tiered-access framework would be a far stronger export, since it is a model that pro-competition regulators globally could adopt without choosing between openness and security, and which will substantially undercut the American argument that EU digital regulation is protectionism dressed as consumer protection.

6. The solution: A tiered-access framework

The question is not whether competition enforcement is warranted or whether Google should be exempt from it. The competition concerns that motivated these proceedings are real. Google's incumbency advantage over rival AI services on Android is documented, and the theoretical case for creating a level playing field is legitimate. The question is whether the mechanism the Commission has chosen – uniform access rights granted to any qualifying third party, without security preconditions, without binding downstream privacy safeguards, and without a revisability mechanism for a technology whose capabilities are changing faster than any specification cycle – is calibrated to achieve that objective without producing collateral harms that the regulation's own parallel frameworks prohibit.

The academic literature surveyed in Section 1 reaches a similar destination from a different direction: Bostoen and Kraemer (2025) argue the DMA needs to be 'adapted thoughtfully and with foresight' for AI agents; Ribera Martínez (2024) argues existing CPS categories can capture AI problems without the adverse consequences of full designation. Both converge on the same practical

---

[25] 'Guarding the gates: The Digital Markets Act and lessons in ex ante regulation', Center for Strategic and International Studies, 5 January 2026 (https://www.csis.org/blogs/charting-geoeconomics/guarding-gates-digital-markets-act-and-lessons-ex-ante-regulation).

[26] 'How do US-Asia trade agreements affect DSTs, FDDEI and VAT?', Bloomberg Law, 7 November 2025 (https://news.bloomberglaw.com/tax-management-international/us-asia-trade-agreements-have-non-tariff-tax-dst-implications-do-not-publish).

conclusion: the current approach is insufficiently calibrated to the risks it entails. A tiered framework is the mechanism for that calibration.

This framework draws on an established precedent. PSD2[27] created graduated API access tiers for open banking, making access to more sensitive financial data conditional on stronger authentication and audit requirements. Telecom interoperability frameworks have long distinguished between basic interconnection and access to sensitive network infrastructure. The principle: access proportionate to demonstrated safeguards, is settled regulatory practice.

Table 1: Proposed tiered-access framework

Tier	Access level	Pre-condition	Governing framework
1	Standard app APIs; no hardware or OS-level access	Standard developer registration only	DMA Art. 6(7) baseline
2	Deep system: Microphone, screen-read, NPU/hardware accelerators, voice triggers, sensors	CRA secure-by-design certification (independent audit required)	CRA + DMA Art. 6(7)
3	Behavioural data: Search signals, query, click/view, usage patterns	GDPR-compliant DPIA; purpose limitation guarantees; auditable retention controls	GDPR + DMA Art. 6(11)

Tier 1: Open and unconditional

Standard, documented APIs that do not provide access to hardware accelerators, system microphones, screen content, or sensor arrays should be available to all third-party AI service providers through normal developer registration. This access will enable most legitimate AI assistant functionality and create a genuinely open baseline without security preconditions that could become barriers to entry for smaller competitors.

Tier 2: Deep system access, conditioned on CRA certification

Access to microphone input, screen-reading APIs, always-on voice trigger capabilities, NPU interfaces, and sensor arrays should be conditional on CRA's secure-by-design certification, an independently verifiable, objective standard. This directly resolves the DMA–CRA conflict by ensuring that access the rights the DMA mandates are granted only to parties meeting the security standards the CRA requires. It also addresses the autonomous agent problem: as AI capabilities shift, certification requirements can be updated to reflect the risks of agentic deployment without reopening the full specification proceedings.

Tier 3: Sensitive data access, conditioned on GDPR compliance

[27] PSD2 is the Second Payment Services Directive, an EU regulation that came into force in 2018 and governs payment services and electronic transactions across the European Economic Area.

Access to search signals under Art. 6(11) should require a completed Data Protection Impact Assessment (DPIA)[28] covering re-identification risks; documented purpose limitation guarantees with audit rights; contractual commitments on retention periods and prohibition of onward sharing; and deletion requirements upon licence termination. Under the GDPR, organisations sharing personal data at this scale are already required to undertake most of these steps. Making them a precondition for access ensures they are fulfilled before data sharing begins.

7. Policy recommendations

For the European Commission and the EU parliament

- **Incorporate tiered access into preliminary findings** by April 2026. The draft specification should distinguish app-level, system-level, and sensitive data access, conditioning each tier on the safeguards described in Section 6.

- **Pause Art. 6(11) data sharing pending implementing acts.** Do not require Art. 6(11) data sharing at scale until binding implementing acts establishing downstream privacy safeguards are adopted. Sharing mandates should not precede the safeguards that make sharing safe.

- **Build a revisability mechanism into the AI specification decision.** An automatic review clause triggered by significant AI capability shifts, defined in consultation with the European Union Agency for Cybersecurity (ENISA) and the European AI Office, should be instituted, to avoid a new full specification proceeding each time the technology changes.

- **Require transparency on cybersecurity consultation.** Document and publish all cybersecurity agency inputs before any final decision is adopted. Apple's observation that security agencies were 'nowhere to be found' in prior DMA interoperability decisions must not be repeated.

- **Address the OpenAI designation gap.** Commission a formal analysis of the OpenAI designation gap. Proceedings that mandate openness from Google's AI infrastructure while leaving its most direct AI competitor entirely outside the DMA's scope risk undermining both the competition and legitimacy objectives they are designed to achieve.

- **Use the specification to defuse, not escalate, transatlantic tensions.** Engage the US administration on the tiered-access framework as a model for bilateral AI platform regulation. A specification incorporating security preconditions would substantially undercut the American 'protectionism' critique and provide a basis for transatlantic alignment rather than trade war.

- **Commission a regulatory coherence study.** Commission a dedicated European Parliamentary Research Service (EPRS) study on the regulatory coherence of DMA Art. 6(7), the CRA, the GDPR, and the AI Act, as they apply to AI platform access.

- **Scrutinise designation asymmetry.** Scrutinise the gatekeeper designation asymmetry and formally ask the Commission to explain why no Chinese platform operating in EU markets has been designated, and what criteria would lead to such a designation in the context of AI services.

[28] DPIA is a process required under Art. 35 of the GDPR. Before carrying out a type of data processing that is likely to result in a high risk to individuals' rights and freedoms, an organisation must conduct a structured assessment of the privacy risks involved and how they will be mitigated. It is not a one-time checkbox but a documented analysis that must be reviewed and updated when the nature of the processing changes.

For national regulators and data protection authorities

- **Issue formal anonymisation guidance before preliminary findings.** Germany's BfDI[29] and France's CNIL[30] should issue formal guidance on what anonymisation standards they will accept for Art. 6(11) data sharing before the Commission's preliminary findings are published. The current absence of operational anonymisation standards for search query data creates compliance uncertainty that serves neither gatekeepers nor data subjects.

- **Submit formal cybersecurity opinions.** National Cybersecurity Certification Authorities (NCCA) should submit formal opinions to the Commission on the system-level access risks identified in Section 2 before any final specification decision is adopted. Security considerations must be part of the specification record.

8. Conclusion

The European Commission's DMA specification proceedings against Google are likely to be the most consequential platform regulatory action of the AI era. They will define what 'effective interoperability' means for AI systems, how behavioural data must be shared while respecting privacy, and what security conditions (if any) must be met before deep system access is granted to rival AI services. The precedent will extend to every gatekeeper and every jurisdiction that follows the Brussels model.

Proportionality is not a weakening of the DMA's objectives. It is a condition for achieving them. A tiered-access framework with access rights determined by compliance with security and privacy standards would open the Android AI ecosystem to genuine competition, respect the EU's own cybersecurity and data protection standards, provide a regulatory model that other jurisdictions can adopt without choosing between openness and security, and answer the most legitimate part of the American critique. It would also create a framework capable of adapting to the autonomous agents that will be the dominant form of AI deployment before this specification's ink is dry.

The Commission has six months and a choice: adopt a proportionate framework that makes the EU a credible, consistent voice in global AI platform regulation, or adopt an ill-calibrated one that hands its critics, in Washington, Beijing, and Brussels, exactly the evidence they are looking for.

[29] Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, or Federal Commissioner for Data Protection and Freedom of Information. It is the national data protection authority responsible for GDPR enforcement at the federal level in Germany.

[30] Commission Nationale de l'Informatique et des Libertés is France's national data protection authority, one of the most active and influential DPAs in the EU, which is responsible for GDPR enforcement in France.

References

Bostoen, F. & Kraemer, J. (2025) How future-proof is the DMA? A case study of AI agents. *SSRN* (https://ssrn.com/abstract=5884302).

Centre for Information Policy Leadership. (2024) Data sharing obligations under the DMA: Challenges and opportunities. Centre for Information Policy Leadership. (https://www.informationpolicycentre.com/wp-content/uploads/2024/05/data_sharing_obligations_under_the_dma_-_challenges_and_opportunities_-_may24.pdf).

Official Journal of the European Union. (2024) Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) European Parliament and Council (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847).

Ribera Martínez, A. Generative AI in check: Gatekeeper power and policy under the DMA. *SSRN* 13 (https://ssrn.com/abstract=5025742).