Comments on the First Review of the Digital Markets Act

Fiona Scott Morton, Alissa Cooper, Jacques Crémer, Amelia Fletcher, Paul Heidhues, Giorgio Monti, Rupprecht Podszun, Alexandre de Streel, Tracy Xu

Table of Contents

1. Introduction

This article is organised into two main parts. In sections 2-4 we provide an account of the design and implementation of the DMA, including lists of enforcement actions and their results to date. The second part of the article gives our recommendations for reforms to DMA implementation. Readers familiar with the DMA are invited to skip to the recommendations in section 5, beginning on page 11.

The European Commission has launched the first statutory review of the Digital Markets Act (DMA), planning to publish its final assessment by May 3, 2026. The Commission's review mandate is to determine whether the DMA remains *fit for purpose*, that is, whether it continues to address the problems it was designed to solve: limited contestability, unfair gatekeeper practices toward business users, and persistent legal uncertainty for market participants.

In this comment, we briefly describe the state of enforcement as of the end of 2025. We then offer a number of recommendations, some larger and some smaller, for underutilized opportunities in the

law, particular compliance challenges, and directions we encourage the Commission to pursue. We offer this comment as a group of European and American economists, lawyers, and technologists sharing a compilation of recommendations. Our list is neither exhaustive nor exclusive. While each of us may vary in the details of implementation of these recommendations, we all agree they are important avenues for the Commission to pursue in order to develop contestable and fair digital markets.

2. Background on the DMA

The adoption of the DMA marked another pivot to regulation within a longer regulatory trajectory in European economic governance.[1] Over the past three decades, the European Union has repeatedly faced markets in which ex post competition enforcement proved too slow or uncertain to discipline structural power. In sectors such as telecommunications, energy, and payment systems, the Commission initially relied on antitrust actions under Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU) but ultimately concluded that persistent market failures required ex ante regulatory regimes.[2] The shift from competition enforcement to rule-based oversight in these sectors reflected a pragmatic recognition: some markets are structurally prone to dominance, and competition litigation is not the right tool to obtain the benefits of rivalry for broader society, perhaps because of the speed of change in the markets, economic drivers of concentration, and/or the insufficiency of antitrust remedies to address competition problems.

Over the 21st century, it has become increasingly clear that digital markets fall into this category. Network effects, economies of scale in data, self-reinforcing dominance, and behavioural frictions that conventional enforcement could not unwind are all manifest in digital platforms. Cases such as *Google Shopping* (2010–2017) and *Android* (2013–2018) illustrated both the reach and the limits of antitrust action: years of investigation did not restore contestability. Between 2017 and 2021, Commission's Directorate-General for Competition (DG COMP) imposed more than €10 billion in fines on large technology companies, yet none of the remedies, from choice screens to revised contractual terms, meaningfully altered market structure. By the time fines were imposed, user habits, developer ecosystems, and advertising networks had already locked in. A 2020 OECD review

[1] For another take on the relationship between the DMA and competition law see Crémer, J. (3 Nov. 2025) "Why you should think of the DMA as competition law" *Concurrences*, 2025/11, Art. N° 129339, https://www.concurrences.com/en/review/issues/no-11-2025/libres-propos/why-you-should-think-of-the-dma-as-competition-law.

[2] For energy, see Commission Communication COM(2006)851 (Energy Sector Inquiry – final report), pp. 1-2, on the need to add regulation to competition enforcement, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM%3A2006%3A0851%3AFIN%3AEN%3APDF. For telecoms, see Directive 2002/21/EC (Framework Directive), on the implementation of regulation in a liberalized telecoms market, https://eur-lex.europa.eu/eli/dir/2002/21/oj/eng. For payment systems, see Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions, paras. 9-16, 33, 37, 40, on the relationship between competition and regulation, https://eur-lex.europa.eu/eli/reg/2015/751/oj/eng.

concluded that "remedies addressing digital gatekeepers have tended to be slow, narrow, and insufficiently forward-looking."

This enforcement fatigue also coincided with a broader recognition that the structure of digital markets has implications extending beyond consumer welfare. The European Digital Strategy of 2020 formally linked competition to innovation, resilience, and technological capacity within the Union. But at the time, few truly believed this was an attainable goal. Only in the mid-2020s did the idea of fostering homegrown innovation gain political and economic urgency, as Europe's dependence on non-European digital infrastructures became evident. In this context, the DMA emerged not merely as a response to market failures but as a cornerstone of Europe's effort to build the conditions under which its own firms can innovate and compete globally.

Rather than revising competition law, the DMA deliberately creates a complementary rule-based regime that applies ex ante. At a general level, the DMA has two normative goals:

- **Fairness** ensures that business users and consumers capture value proportional to their contribution. When platforms impose discriminatory terms or extract data rents, value distribution becomes unfair even if prices appear to be zero.
- **Contestability** secures the possibility for rivals to enter and innovate without facing structural exclusion. It is the dynamic complement to fairness: without entry, fairness cannot be sustained.[3]

In practice, the DMA imposes defined obligations and prohibitions on designated "gatekeeper" platforms and avoids the hurdles that antitrust enforcement faces including market definition and the need to prove dominance, anticompetitive conduct, and consumer harm in each individual case. Every obligation ultimately seeks either to canalize gatekeeper control over access (fairness) or to reduce switching and entry barriers (contestability). Additionally, the participative and deliberate nature of sectoral regulation in the DMA means that the evidentiary standard it faces on judicial review is more deferential than under antitrust.

The DMA attempts to create quicker and more certain progress from entrenched digital platforms to competition that helps European businesses and consumers. If this ambition is realized, the DMA will realign incentives, redistribute bargaining power, and ensure that the digital economy remains an open environment for entrepreneurship and technological progress.

3. Assessing the DMA

The Commission's review must assess the degree to which the Act has achieved its objectives of ensuring contestable and fair markets for digital platform services, its impact on business users and end users, and whether any further measures are necessary to guarantee effectiveness. The review must also examine opportunities for reducing unnecessary administrative burden. At the same

[3] Crémer, Jacques, et al. (2023) "Fairness and Contestability in the Digital Markets Act" *Yale Journal on Regulation*, 40:923–1012.

time, it will consider whether the framework is robust enough to address new challenges, for example, those posed by AI-powered services.

The Commission has framed the review as a consultative and evidence-driven process. Stakeholders, including business users, SMEs, consumer organisations, and academics, have been invited to submit qualitative and quantitative evidence on how the DMA has affected market dynamics. Over 450 comments have been submitted and are summarized by the Commission here. The summary emphasizes the experience of SMEs who are the entities that rely most heavily on gatekeeper platforms for market access, but also provides the gatekeepers' perspectives on each issue. However, the review must take into account that obligations have been applicable for only a short period and therefore making definitive conclusions at this stage is difficult. The challenge, therefore, is to combine early evidence with forward-looking evaluation.

This will be the first formal review of the law since the DMA entered into force in November 2022 and became fully applicable in March 2024. For Europe's broader policy landscape, the review carries strategic implications. It will signal whether the EU remains committed to its model of ex ante competition regulation in an environment where the bloc faces pressures to reduce the regulation it places on large firms. To the extent that the report explains what has worked and what improvements are needed, other jurisdictions can learn how the DMA best serves as a template for digital governance in their nation.

At the same time, emerging technologies are redrawing the boundaries of intermediation. Generative-AI systems and conversational agents increasingly mediate how users search, shop, and interact with online content. If such systems are deployed by gatekeepers, they may perform functions analogous to search engines or app stores, raising questions about the DMA's definitional scope. Similarly, the growing concentration in cloud infrastructure markets suggests that switching and interoperability issues may soon resemble those of operating systems. The 2026 review offers an opportunity to assess whether the DMA remains adequate for an AI-integrated economy.

Our objective with these comments is not to be comprehensive, but to make what we hope are useful observations that assist policymakers in improving DMA enforcement, laying the groundwork for fair, contestable, and resilient digital markets in Europe.

4. DMA Enforcement in Brief: 2022 - 02/2026

At its core, the DMA shifts Europe's approach from liability rules to entitlement rules. Instead of requiring regulators to prove abuse ex post, the Act establishes ex ante duties of conduct for firms designated as gatekeepers—a category defined through both quantitative thresholds (such as €7.5 billion annual turnover in the EEA; 45 million active users) and qualitative criteria of entrenched intermediation. The law also identifies twenty-two core platform services (CPS), ranging from online search and social networking to operating systems, advertising intermediation, and virtual computing services, and imposes constraints (obligations) on the behaviour of the gatekeepers when they provide a CPS. These constraints vary, of course, from CPS to CPS, but are the same for all the designated gatekeepers providing this CPS.

Article 5 sets out *prohibitions*: gatekeepers may not self-prefer their own services, combine personal data across units without consent, restrict business users' steering, or impose anti-competitive bundling. Article 6 introduces obligations susceptible to further specification through dialogue with the Commission, covering interoperability, data access, and transparency. Article 7 adds technical duties to ensure messaging-service interoperability. Together, these provisions represent a move from reactive enforcement toward a market-design regime in which competitive neutrality and openness are built into digital interfaces.

Of course, even given these specific obligations, the law leaves discretion both to gatekeepers and the Commission in interpreting and following the law. Furthermore, Article 8 begins, "The measures implemented by the gatekeeper to ensure compliance with those Articles shall be effective in achieving the objectives of this Regulation and of the relevant obligation." In other words, the gatekeepers are responsible not only for following the letter of the obligations, but also for abiding by their spirit.

The DMA's economic logic recognizes that power in the digital age lies not only in prices or output but in control of interfaces and data flows. The legislation, therefore, rebalances entitlements, granting business users rights to communicate with their customers outside the gatekeeper's ecosystem, for advertisers, rights to audit campaign data, and for end users, rights to uninstall and make default applications. Such rights aim at rebalancing the bargaining between platforms and business users in a way that creates more incentives for innovation and allocates more surplus to business users (and end users).

The DMA also creates a new form of regulatory governance that blends legal constraint with ongoing technical dialogue—an institutional innovation unprecedented in EU regulatory history. Of course, this structure is not without its challenges. In our recommendations below we develop suggestions accordingly, notably around the difficulty of specifying with precision the behaviours the act mandates and forbids, as well as demands of enforcement on a limited staff inside the Commission.

The first enforcement cycle of the DMA unfolded through a sequence of procedural steps that converted the Regulation's ex ante framework into an operational supervisory system. While the DMA presented itself as being largely self-executing, implementation has not met that hope. Early implementation relied on designation decisions, rebuttal investigations, compliance reporting, and targeted enforcement actions that collectively defined how obligations would be interpreted and applied. This section reviews these procedural developments and documents how the enforcement architecture took shape ahead of observable market responses.

4.1 Gatekeeper and Core Platform Service (CPS) Designation

The Commission has acted with notable speed. By late 2024, the DMA regime comprised seven designated gatekeepers and twenty-four core CPSs. Initial designation decisions were adopted in September 2023, identifying Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft as

gatekeepers across twenty-two CPSs. In 2024, the Commission added Apple's iPadOS as an operating-system CPS and Booking.com as an online intermediation CPS[1], expanding both the number of covered services and the range of business models subject to the regime. These designations triggered the six-month compliance period ending in March 2024 for each newly designated service.

Designation practice clarified that the quantitative thresholds in Article 3 operate as rebuttable presumptions, not automatic rules, as illustrated by rebuttal investigations concerning iMessage, Bing, Edge, Microsoft Advertising, X Ads, and TikTok Ads. Several services were ultimately not designated following a qualitative assessment of their gateway role.[2]

Cloud infrastructure services are not currently designated as CPS under the DMA. However, in November 2025 the Commission opened three market investigations on cloud computing services, including two to assess whether Amazon Web Services and Microsoft Azure should be designated as gatekeepers despite not meeting the quantitative thresholds for the number of business users. (A CPS is defined to be an intermediary between business users and end users.) The third investigation examines whether existing DMA obligations are sufficient to tackle unfair practices in cloud markets.[4] These investigations are an excellent use of the Commission's authority under the DMA to investigate an area of broad social and policy concern even when quantitative metrics—by market configuration—are not applicable. The appropriateness of the investigation holds even if the design and challenges of the cloud market ultimately suggest to the Commission that the DMA is not the appropriate tool to address it.

The Commission's designation decisions reflect a functional, ecosystem-oriented approach to CPS classification. Rather than relying on narrow product-line definitions, the Commission has emphasized whether a service plays an "important gateway" role in mediating interactions between business users and end users, including where that role is embedded within a broader ecosystem. This approach allows CPS boundaries to track intermediation functions rather than formal product categories and leaves scope for future reassessment as technical configurations evolve.

4.2 Compliance Reporting and Supervisory Dialogue

The first compliance reports, submitted in March 2024 under Article 11, varied widely in length, structure, and substance. Public versions ranged from roughly a dozen pages to several hundred pages, with confidential submissions extending further, and covered dozens of CPS-specific implementations across the initially designated gatekeepers, as well as subsequent reports submitted later in 2024 following the designation of iPadOS as a covered CPS and Booking.com as a gatekeeper. Many early reports emphasized legal interpretation and general principles rather than concrete descriptions of technical implementation, revealing substantial heterogeneity in how undertakings approached the reporting obligation.

---

[4] European Commission press release (18 Nov 2025) "Commission launches market investigations on cloud computing services under the Digital Markets Act" https://digital-markets-act.ec.europa.eu/commission-launches-market-investigations-cloud-computing-services-under-digital-markets-act-2025-11-18_en.

Over the course of 2024, subsequent submissions generally became more detailed, incorporating descriptions of system architecture, data flows, APIs, default settings, and user journeys. However, there is no consensus that this evolution has made compliance reporting an effective stand-alone tool. Stakeholder submissions summarized in the Commission's Article 53 consultation repeatedly questioned the transparency, verifiability, and practical usefulness of public compliance reports, characterizing them as lengthy justificatory documents that often explain why existing practices are claimed to be compliant rather than providing testable accounts of how obligations operate in practice.[5] No formal reporting template has been issued by the Commission; any convergence in structure reflects iterative supervisory dialogue rather than a standardized framework.

In practice, compliance reports have functioned primarily as inputs into enforcement, rather than as an enforcement mechanism in their own right. The Commission has used them as a starting point for further requests for information, technical workshops, and ultimately specification or non-compliance proceedings. The public versions of compliance reports have also varied. While some gatekeepers published redacted public summaries, others disclosed little. Few end users, business users, scholars, or policy analysts have found the reports particularly helpful or illuminating. This pattern reflects a broadly shared assessment that compliance reports (of this type) alone are insufficient to ensure effective implementation, particularly given gatekeepers' incentives for strategic or minimal compliance.

4.3 Non-Compliance Proceedings

Following review of the initial compliance reports, the Commission opened its first DMA non-compliance proceedings in March 2024, targeting specific CPS-level obligations rather than entire business models. Table 1 (below) summarizes all publicly known DMA non-compliance actions to date, including their legal basis, timing, and procedural status.

By April 2025, the Commission adopted its first non-compliance decisions, imposing fines on Apple and Meta. These early cases illustrate how the Commission interprets the boundary between imperfect or incomplete compliance and actionable infringements. Investigations focused on whether the implemented measures delivered effective user choice and business-user access, not simply on whether they could be reconciled with a literal reading of the text.

Recurring issues included the design of choice screens that formally offered alternatives but relied on multi-step flows, warnings, or default nudges; and security-based justifications for limiting sideloading or alternative app stores. In the context of noncompliance proceedings in response to these violations, the Commission has chosen to engage in lengthy negotiations with platforms. In the case of the self-preferencing investigation against Google, the Commission has extended these negotiations well past the statutory framework of announcing noncompliance decisions within a year of the start of the investigation. It remains an open question whether such conversations will produce compliance. The Commission has also engaged in negotiations and dialogue outside of the framework of noncompliance (or, see below, specification) proceedings.

Table 1: DMA Article 29 non-compliance proceedings to date (public record)

Gatekeeper	**CPS concerned**	**Obligation(s)**	**Proceeding opened**	**Procedural Status**	**Outcome/Key points (as of early 2026)**
Alphabet (Google)	General Search	Art. 6(5) (self-preferencing)	March 2024	Investigation ongoing (no final decision as of early 2026)	Concerns focus on ranking and treatment of own services and treatment of rival vertical services in search results.
Alphabet (Google)	Google Play (App Store)	Art. 5(4)(steering); Art. 6(3) (choice architecture)	March 2024	Investigation ongoing (no final decision as of early 2026)	Commission assessing effectiveness of implemented steering and alternative billing measures.
Apple	App Store (iOS)	Art. 5(4) (steering); Art. 6(3) (choice and access conditions)	March 2024	Non-compliance decision adopted (April 23, 2025)	Commission found Apple in breach of anti-steering obligations; €500 million fine imposed; compliance period set; further aspects (e.g. new business terms) still under review
Meta	Social networking /advertising	Art. 5(2) (data combination; consent)	March 2024	Non-compliance decision adopted (April 23, 2025)	Commission found Meta non-compliant for failing to provide equivalent consent alternatives; €200 million fine imposed; revised personalized-ads model remains under review

4.4 Specification Decisions

Specification proceedings under Article 8 occupy an intermediate position between supervision and sanctioning. The Commission has the authority to start a procedure for "specifying the measures that the gatekeeper concerned is to implement in order to effectively comply with the obligations laid down in Articles 6 and 7" (Art. 8(8) DMA). The function of the proceeding is to clarify ambiguous obligations, reduce information asymmetries between regulators and gatekeepers, and promote a degree of consistency across ecosystems where similar obligations apply to different

technical architectures. In contrast to non-compliance proceedings, specification does not incorporate a finding of infringement; it allows the Commission to intervene prospectively where obligations require specific technical implementation. Specification decisions are also time-limited to six months, which has held the Commission and gatekeepers to a tight timeline.

In March 2025, the Commission adopted two formal specification decisions concerning Apple under Article 6(7). These decisions addressed, first, interoperability between Apple operating systems and connected devices, and second, the procedures governing third-party requests for interoperability access. Rather than imposing penalties, the specifications set out detailed technical and procedural requirements intended to make interoperability effective and verifiable.

In January 2026, the Commission opened specification proceedings concerning Google's implementation of Article 6(7) (interoperability) and Article 6(11) (online search data access). These proceedings remain ongoing and do not constitute a finding of non-compliance. Table 2 lists all publicly adopted and ongoing specification proceedings.

4.5 Monitoring and Institutional Capacity

Alongside these core procedures, the Commission has built a broader monitoring and evidence-gathering architecture that draws on third-party input, technical audits, and cooperation with national regulators, controlled experiments, and reverse-engineering of user flows. The Commission's annual reports emphasize the growing reliance on specialized engineering and data-science expertise to evaluate compliance claims and to design and test appropriate remedies.

Resource constraints further shape enforcement strategy. Individual gatekeepers command engineering and compliance teams that far exceed the Commission's technical capacity, limiting the feasibility of continuous, system-wide monitoring. This imbalance helps to explain the Commission's reliance on iterative engagement, targeted non-compliance proceedings, and specification decisions rather than sweeping, one-off interventions. It also underscores a recurring concern expressed in the consultation process: that monitoring and dialogue, while necessary, cannot substitute for timely and credible enforcement if the DMA's objectives of fairness and contestability are to be realized in practice.

By late 2025, the DMA's enforcement architecture had developed a layered system: designation defines scope, compliance reporting structures implementation, non-compliance proceedings test effectiveness, and specification resolves technical ambiguity. These instruments, supported by ongoing monitoring and third-party input, form the institutional backdrop against which market outcomes must be interpreted. The next section examines how these enforcement practices and compliance strategies are shaping contestability, entry, data access, and user choice in EU digital markets.

Table 2: DMA Article 8 Specification Decisions to Date (public record)

Gatekeeper	CPS concerned	Obligation(s)	Proceeding opened	Procedural Status	Outcome/Key Points (as of early 2026)
Apple	iOS (Operating System)	Art. 6(7) – interoperability with connected devices	September 2024	Specification decisions adopted (March 19, 2025)	Specification clarified technical and procedural requirements for interoperability between iOS and third-party connected devices, including documentation, access conditions, and timelines.
Apple	iOS (Operating System)	Art. 6(7) – third-party interoperability requests	September 2024	Specification decisions adopted (March 19, 2025)	Specification established a structured process for handling, assessing, and responding to third-party interoperability requests, aimed at making access verifiable and enforceable.
Alphabet (Google)	Android/AI service interoperability	Art. 6(7) – interop with hardware/ software features used by Google's own AI services	January 2026	Specification proceedings ongoing (as of early 2026)	Commission opened proceedings to "assist Google in complying" with Art. 6(7), clarifying scope and implementation of interoperability; no non-compliance finding or fines, with final specification decisions expected within six months of opening.
Alphabet (Google)	Google Search/AI data-sharing conditions	Art. 6(11) – search query/click data sharing on FRAND terms	January 2026	Specification proceedings ongoing (as of early 2026)	Commission opened proceedings to "assist Google in complying" with Art. 6(11), clarifying scope and implementation of anonymized search data sharing obligations; no non-compliance finding or fines, with final specification decisions expected within six months of opening.

5. Recommendations in Review[5]

5.1 Benchmarking Design with Civil Society and Independent Auditors

The process by which a gatekeeper establishes that it is in compliance with the DMA badly needs improvement. In particular, the Commission should be using rigorous standards to evaluate gatekeeper designs and algorithms and how they influence user choices. Because checking every choice point is beyond the capacity of Commission resources, the DMA enforcement process must do better at leveraging outside resources. Because the recommendations in this section all fall within the bounds of the DMA's compliance requirements, the Commission should not require legal amendments to implement improvements similar to those suggested.

Any assertion made by the gatekeeper that it has complied with DMA requirements for interoperability, choice architecture, algorithm, data portability, real-time data feed, etc. must demonstrate that compliance with an audit by an independent third party who meets conventional professional standards and is hired at the gatekeeper's expense.[6] Such an audit would require the auditor to have substantial access to gatekeeper documents and engineers, records of A/B testing, live protocols, and more. The independent auditor must certify that they have tested the services offered to end users and business users and that those services work as described. The gatekeeper will observe whether it meets the auditor's standards as the process unfolds and therefore have certainty about its compliance. In addition to reviewing changes to gatekeeper practices, the auditor should also describe the end user and business user journey – technological or legal hurdles, scare screens, and the like - required to make the services work as described.

The changes the DMA requires are significant; and as these changes will often reduce the gatekeepers' profits, absent a meaningful review of compliance by the Commission, gatekeepers will have an incentive to not fully comply. In some cases, business users are able to assess compliance, but in others they may not have enough visibility or data to reach a conclusion. Business users may also be afraid of retaliation from the platform. Compliance reports are insufficient for civil society to assess compliance. For these reasons, verification of the gatekeeper's changes must be carried out by a third party. The Commission does not have the resources or expertise, and therefore a neutral expert third party is needed.[7]

---

[5] A number of authors have coauthored other recommendations, some submitted as part of the formal comment period. Some of those recommendations are repeated here, but we encourage the review of all of them. For some examples, see, Andriychuk, O. et al (2025) "Consultation on the 2025 Review of the Digital Markets Act (DMA)" *SSRN*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5528062; Feasey, R., Monti, G., de Streel, A. (2025) "Policy Recommendations to Improve DMA Process and Institutions" *CERRE*, https://cerre.eu/wp-content/uploads/2025/03/DMA-Recommendations_FINAL.pdf and "DMA@1: Looking Back and Ahead" *CERRE*, https://cerre.eu/wp-content/uploads/2025/03/DMA@1-Looking-Back-and-Ahead_Final.pdf.

[6] Interoperability continues to be a central focus of compliance efforts in a range of dimensions (see also below at 5.6). We have previously articulated more robust framings for such efforts. *See* Scott Morton, F., et al (2023) "Equitable Interoperability: The 'Supertool' of Digital Platform Governance" *Yale Journal on Regulation*, 40/3, https://www.yalejreg.com/print/equitable-interoperability-the-supertool-of-digital-platform-governance/.

[7] Article 26 para. 2 of the DMA mentions the Commission's ability to rely on hired auditors to assist in its monitoring and compliance work.

As part of this review, it is particularly important that claimed compliance relating to choice architecture should be evidenced by A/B testing carried out by the gatekeeper. The auditor will assess this testing but should not need to carry it out themselves. Moreover, the gatekeeper must include sufficient data and experiments to show its choice architecture is neutral and non-exploitative in both the public and confidential compliance reports. The auditor of these experiments should have experience in designing experiments and in best-practice methodology for carrying out such experiments. For example, a gatekeeper should not run 1000 experiments and report only the most favourable three to the Commission. An expert in experimental methods who is employed as an auditor would likely require the gatekeeper to keep a log of all its experiments so that those being reported can be compared to those that are not.

Of course, the selection and evaluation of auditors is itself a critical function of the Commission. Some standard of certification should be required, perhaps designed by the Commission. (Public bodies routinely approve and run auditors, such as Luxembourg's Court of Auditors, and could advise the Commission on such design.) The Commission will also need to create standards for audits that clarify the auditor's responsibilities and limits. Auditors will not relieve the Commission, the gatekeepers, or civil society from the need to evaluate the substance of the compliance solutions. But auditors are helpful in evaluating whether the implementation of gatekeeper promises and commitments matches what it has stated it has done in those commitments (e.g., if the gatekeeper has committed to allowing third party app stores, does the actual process for a user or developer who wants to download, start, or interface with such a store live up to the commitment, and has the gatekeeper demonstrated as much). And because an auditor has access to confidential information and data, it is able to confirm gatekeeper testing procedures and any empirical statements the gatekeeper provides as part of its compliance report.

For their own accountability, auditors, too, should issue public reports describing the methodology and standards they apply without disclosing privileged information. And of course the gatekeeper's internal compliance officer required by the DMA will continue to have the responsibility to certify that the compliance report is complete.

Civil society, too, has a role to play in accountability and the achievement of better DMA compliance. Substantive (see below) compliance reports, testing results, and other data made available within the limits of privacy, security, and IP concerns will all enable public experts to study and evaluate compliance efforts.

Two areas that could benefit from civil society contributions are already evident. First, centres of expertise such as universities, consumer organizations, etc. could evaluate and propose best practices for choice architecture: designs or design principles that enable but protect accurate consumer choice. Of course, the credibility of these institutions would itself be dependent on funding transparency, reputation, and public recognition. Work from credible institutions, however, could form the basis for a set of best practices the Commission could adopt to create a "safe harbour" for gatekeepers. Then the Commission need not assess every choice screen of every gatekeeper every year. Rather, the gatekeeper could certify that it had adhered to the

recommended design principles, subject to verification by the auditor. If the auditor agreed that the correct standards were applied, the gatekeeper's choice architecture could be immediately determined to be in compliance with the DMA without necessitating further investigation by the Commission absent unusual circumstances.

The second area of demand is the development of standards for evaluating algorithms. The question of whether an algorithm has been designed, or has learned, to be biased in favour of the gatekeeper is critical to gatekeeper compliance. This is a less well-researched area and needs public investment to generate useful methods for assessing the performance of an algorithm. Universities, think tanks, and other parts of civil society could work on methods such as sandboxes, populated with data constructed to have certain properties, that could be used to test an algorithm. A third-party auditor who is hired to evaluate the gatekeeper's claims of algorithmic neutrality could use the best-evidenced tools and methods to verify gatekeeper compliance (it may be necessary for the Commission itself to standardize, as above, a set of tools or practices). If neither the auditor nor the gatekeeper used these methods, a heavier burden of empirically demonstrating compliance would be on the gatekeeper. In particular, the gatekeeper would be required to publish publicly the full data and methods it used in its reported process of demonstrating compliance. With these methods and data, outside parties and researchers could evaluate whether the gatekeeper's process was flawed.[8]

5.2 Compliance Reports

Overall, the annual compliance report is currently an underutilized tool in achieving and assessing compliance. In the compliance report, gatekeepers are meant to explain how they adhere to the DMA and fulfill its obligations, which necessarily requires providing information on contestability. Potential entrants or competitors that want to make use of data-sharing or interoperability requirements need detailed information on how – in practice – they can make use of the gatekeepers' compulsory offers. Useful compliance reports should include (or direct business users to) explanations of the exact requirements and procedures for building, interoperating, receiving data, and so forth. Indeed, unless such information is made available publicly, we do not think a gatekeeper is fully compliant. Furthermore, compliance reports need to demonstrate that gatekeepers have fulfilled their obligations by having an auditor confirm that the process works from the perspective of the business user.

It is important that compliance reports can be scrutinized, by the public and (potential) business users that are meant to benefit from the fairness and contestability that the DMA is attempting to achieve. Hence, the public reports should be as detailed as possible, and details relegated to the confidential versions only if absolutely necessary.[9] The more is made public, the better independent researchers or competitors can ensure that the reports are truthful and not misleading—which

[8] We further discuss evidencing compliance in our 2024 article, Fletcher, et al (2024) "The Effective Use of Economics in the EU Digital Markets Act" *Journal of Competition Law & Economics*, 20/1-2, https://doi.org/10.1093/joclec/nhad018.

[9] See Andriychuk, O. et al (2025) (supra n. 5) for further discussion of compliance reporting and third-party compliance evaluation broadly relevant in this section and others.

would have the additional benefit of holding auditors themselves responsible to public scrutiny. The Commission should require that only limited sensitive facts be withheld, and only for a limited time. Since these markets are dynamic, standard practice should be to release more details after some time has passed. The earlier the initially-withheld information becomes publicly available the better.

A useful revision of the DMA would establish that insufficiently detailed or incorrect compliance reports should be considered as being non-compliant with the DMA as well as trigger fees that run daily while the important information is withheld or not clearly explained. The Commission should explore simple mechanisms to identify incomplete compliance reports, as these can then create a presumption of non-compliance (until the gatekeeper rectifies the report with more detailed information). Currently, the commission lacks an effective way of enforcing non-cooperating gatekeepers to provide useful reports. One approach could be for the Commission to provide feedback on each report describing any shortcomings and what they expect to see the next year. If the gatekeeper does not provide the requested information the next year, the gatekeeper would not be in compliance, and a substantial fine would be justified in light of the long lead time and specific instructions.

In line with the theme of many of our recommendations, the Commission should refine a template for the compliance report that both allows comparisons from year to year and also serves as a safe harbor for gatekeepers. (The Commission has already published a kind of template available online, although it more closely resembles a list of requirements rather than a structured report.) In such a template, the public version should be a line-by-line redacted version of the full report to allow the public to understand the scope, shape, and volume of the redacted information contained in the report, even though the content cannot be seen publicly. The Commission should also host all past compliance reports on its own website so that these continue to be available to the public in perpetuity.

5.3 Key Performance Indicators (KPIs)

In order to gauge what the DMA achieves, it would be useful to have output indicators that reveal the extent to which end users and business users have engaged with the opportunities that the DMA is intended to introduce. Such indicators should be developed for each obligation. Some of us have previously described in much greater detail how such indicators may be developed.[10] These data points are a first step to understanding what choices stakeholders make. These data could be used in multiple ways: they could (a) indicate whether a gatekeeper is complying (e.g., by comparing data across gatekeepers subject to the same obligation); (b) indicate whether an obligation is working well; (c) signal if an obligation is unnecessary because there is no user demand; (d) flag an obligation that needs to be improved. If a gatekeeper failed to include identified indicators in its compliance report, it would be deemed to be noncompliant.

[10] Feasey, R., de Streel, A. (2024) "DMA Output Indicators" *CERRE*, https://cerre.eu/wp-content/uploads/2024/01/DMA-Output-Indicators_FINAL.pdf.

Such indicators should be specified by the Commission but may be collected and analysed by other entities to advance understanding of compliance. For example, a civil society foundation could record entrants in a given market and evaluate the impact on competition. Third parties may be helpful in finding KPIs and flagging ones trackable with public data, though in many cases, the gatekeepers themselves will be the appropriate actors. AI tools may themselves be useful for compiling and tracking large-scale data. With respect to confidentiality, with time, data reported to the EC on the basis of confidentiality may become less confidential, enabling its integration into these metrics.

The current review of the DMA is likely too early to incorporate substantive output indicators into evaluation, but future evaluations of the efficacy of the law (i.e., one scheduled for 2029) should include impact as a critical part of evaluation, including the costs and benefits of various obligations and implementation efforts. As these metrics mature, they will help to clarify the requirements of effective compliance, creating greater certainty and stability for gatekeepers and business users alike. Such an evidence-based approach to enforcement and evaluation will be critical to ensuring the law delivers on its objectives.

5.4 Article 7: Interoperability in Number-Independent Interpersonal Communication Services

Unique among the DMA obligations, Article 7 was designed to promote horizontal interoperability in number-independent interpersonal communications services (NIICS). Messaging, voice, and video services have long been promising candidates for horizontal interoperability due to their mature technical foundation and a high degree of functional alignment across platforms. Deployed services frequently make use of established standards, published protocols, and shared software libraries. Their core interaction designs—sending, receiving, calling—are very similar across the industry. Furthermore, many of these services rely on service-independent identifiers, such as phone numbers and email addresses, which provides a relatively robust starting point for resolving cross-service identity and addressing challenges. All of these features make interpersonal communications services good candidates for horizontal interoperability in theory.

In practice, two years into the DMA's implementation, Article 7 is functioning more like a vertical interoperability provision – and one that has seen negligible take-up in the market. This outcome is the result of a compounding set of factors.

First, the Commission designated only a single NIICS gatekeeper, Meta. Had other NIICS undertakings been designated as gatekeepers, the landscape of both the gatekeepers' reference offers and the appetite for interoperability uptake among competing businesses could have been significantly different. On the gatekeeper side, having multiple gatekeepers subject to compliance obligations would have created an incentive for the Commission to encourage harmonization in reference offers and interfaces across gatekeepers. On the competitor side, the opportunity to interoperate with more services and more users by implementing a single set of software or architecture changes could have created a stronger market imperative for competitors to take up the reference offers.

Second, the Commission designated only two core platform services, WhatsApp and Facebook Messenger. In the marketplace, Facebook Messenger is effectively a closed platform – unlike many other messaging services that support finding users by phone number or email address, Messenger users are only reachable via Facebook accounts. Facebook Messenger does not interoperate with any of Meta's other messaging products (WhatsApp, Instagram Direct Messages, or Threads). Under these circumstances, it is unsurprising that no competitors have deployed products that interoperate with Facebook Messenger on the basis of the DMA reference offer.

That leaves WhatsApp as the main target for interoperability. Meta has been free to design its reference offer as it chooses, in accordance with the security, privacy, and user choice requirements of Article 7. As such, from a competitor's standpoint, what Article 7 amounts to in practice is access to WhatsApp users on WhatsApp's terms – potentially quite a similar result to what a vertical interoperability provision would have yielded (since WhatsApp is the only in-demand designated service, there is no possibility for real horizontal interoperability between a number of different designated services).

The evidence in the market, resulting from the combination of the institutional design of Article 7 and implementation choices made by the Commission, bears directly on the question of how well Article 7 is servicing the goals of the DMA, particularly contestability. For NIICS to be contestable, there must be enough users whose choice of provider is contestable – i.e., enough users willing to adopt a new rival's service, switch to a competitor, abandon the gatekeeper's service, or some combination of these behaviours. Vertical interoperability only directly facilitates the first of these, whereas horizontal interoperability potentially facilitates all three.

The market response to Article 7 to date demonstrates this in practice. Two small, early-stage start-ups, BirdyChat and Haiket, have announced that they are making use of WhatsApp interoperability. BirdyChat bills itself as a messaging service for professionals, while Haiket provides a voice interface to chat functionality. Neither product is broadly available to the public, neither brands itself as a WhatsApp substitute, and neither should reasonably be considered a horizontal competitor to the general-purpose WhatsApp service. Larger WhatsApp competitors have either not pursued interoperability or abandoned their plans due to lack of business viability. What these rivals stand to gain for the cost of implementing interoperability is not worth it from a contestability perspective. As such, the factors described above that have shaped outcomes under Article 7 have collectively narrowed the impact of the DMA's contestability improvements in this market.

As the Commission considers proposals to extend the Article 7 obligations to social media, the primary lessons to be drawn from the experience of Article 7 thus far related to the design of obligations together with their implementation. Interoperability requirements must be crafted with close attention to the business realities of the market at issue and the incentives that regulated undertakings will have to create barriers to interoperability through their implementation choices. The market being technologically ripe for horizontal interoperability, as NIICS services are, is insufficient on its own for this form of interoperability to materialize. What kinds of businesses

would seek interoperability? How would they make the business case? What would the user experience of interoperability be like? What would be users' incentives to adopt an interoperable offering? Detailed scenario planning that maps proposed requirements to anticipated outcomes in the covered market is needed to justify the specific approach taken to any interoperability mandate the Commission may consider, now or in the future.

5.5 Possibilities for and Appropriateness of Regulating AI under the DMA

The development and implementation of AI have progressed rapidly over the last two years. In some ways, the implications for competition have so far been positive, with a number of major new players (OpenAI, Anthropic) and a myriad of smaller companies emerging. However, outside of China, the DMA-designated companies have invested most heavily in this area.

This investment is valuable and deserves a fair return. However, there is a substantial risk that these firms will be able to use their existing strong market positions to promote their own AI services in an anti-competitive way, where such services have the potential to be competitive. The concerns arising are very similar to those that the DMA already addresses, such as restricted interoperability. A topical example is Meta's WhatsApp removing interoperability for third party chatbots to favour MetaAI, which the Commission is currently investigating under Article 102 TFEU (the Commission recently announced possible interim measures that would provide some immediate redress to the problem). Apple has also so far provided very limited interoperability for AI services relative to Google and Microsoft (with Graph).

To mitigate this risk, we first urge the Commission to use the existing DMA regulatory framework to address these issues, and we see its recently announced specification proceedings as a positive step in this direction. These proceedings are focused on Google's possible preferencing of its Gemini service as positive in this regard and the potential for AI chatbots to constitute search engines under the data sharing provisions of Article 6(ii),

We also urge the Commission to consider whether any AI services merit designation under the DMA, potentially as virtual assistants. We note that this may require qualitative designation under Article 3(8) since the quantitative thresholds for automatic designation may well not yet be met, especially in relation to active business users. Such designation would have immediate benefits. For example, under Article 6(3), Google would then be required to provide a choice screen on Android devices, so that consumers could choose between Google's Gemini and third-party AI alternatives as their default AI service.

We further urge the Commission to carry out a market investigation in this area. This should also consider whether minor revisions are required to any of the rules within Articles 5 or 6. For example, for the DMA to properly address the risks arising from AI to the DMA's objectives, it may be that the existing DMA framework will require minor revisions to properly address the issues arising due to AI. For example, the Meta interoperability issue cited above arguably cannot be addressed under the DMA as it stands. Article 6(7) only requires interoperability with "the same hardware and software features accessed or controlled via the OS or virtual assistant." This is

arguably not relevant to services wishing to interoperate with other designated non-OS services (at least unless MetaAI is also designated as a virtual assistant under the DMA). Likewise, it may be necessary to make a minor revision to confirm that Article 6(11) covers AI chatbots.

At the same time, there may be very significant risks now arising from certain DMA rules that would not have been obvious at the time they were written. For example, Amazon is currently denying access to its retail platform to AI agents, which would appear to be in breach of Article 6(7). However, allowing such access would critically threaten important elements of Amazon's revenue, since AI agents are less likely than humans to be influenced by advertising and rankings. The trade-offs here are subtle and would merit further thought within a market investigation.

6. Conclusion: The Importance of Independence

The critical unexpected aspect of the DMA that badly needs improvement is the extent to which geopolitics has influenced, and weakened, DMA enforcement to date. There is an urgent need for a political conversation about how to insulate enforcement of the DMA so that both citizens get the benefits of the law they voted for, and gatekeepers and business users have legal certainty. We do not have a thoughtful solution for this problem, which is why we raise it only in the conclusion of this report as a topic for immediate discussion by the European Parliament.

The DMA must be structured so that regulators have the capacity to sustain and effectively carry out the enforcement mandate over time, despite legal challenges, resource constraints, political pressure, resistance from regulated actors, and changing conditions. For contestability purposes, it is critical to have reliable enforcement such that business users and gatekeepers alike gain confidence in the stability and strength of the law as well as its protection from political distortions. We provide some creative suggestions in this conclusion to stimulate the debate.

At present, DMA enforcement decisions are taken by the College of Commissioners and therefore enforcement is vulnerable to shifting political priorities. Alternatives that would lessen this problem include creating an independent agency to enforce the DMA (which could also include other enforcement activities of DG COMP). Additionally or alternatively, final decisions could be taken by an independent body (e.g. the court or an independent panel). If centralisation was not favoured, Member States could be encouraged to establish independent, adequately resourced enforcement units to support the effective enforcement of the DMA. If the DMA enforcement team is set up to act independently, it must be independent from political priority setting in the Commission and therefore have access to resources that are not politically controlled. DMA enforcement should have its own budget line and gatekeepers should pay annual fees to fund the enforcement budget.

Another way of inoculating enforcement against capture is to create stable and workable frames for private enforcement in the form of stand-alone claims (cf. the 2025 ruling by Landgericht Mainz). Some possibilities include clarifying the DMA in favour of private enforcement, including revising Article 39; limiting the time frame within which the Commission can intervene in private enforcement; amending Article 39(5) so that courts can always grant interim injunctions, even in

cases where the Commission may become active at a later point; and extending the Damages Directive (2014/104/EU) to cases of DMA infringements to facilitate claims.