The Credibility of the DMA's Compliance Reports

Alba Ribera Martínez*

ABSTRACT

The institutional setting of the Digital Markets Act (DMA)[1] reverses the rationale of the application of Articles 101 and 102 TFEU[2] to make profound changes in digital business models. The deterrence-based framework gives way to an instrument based on cooperative engagement between private and public actors. Private undertakings, termed as gatekeepers, bear the burden of submitting compliance reports to the European Commission detailing their technical implementation of the regulation.

Following the first round of compliance reports submitted by six gatekeepers in March 2024, the paper seeks to clarify their role as stemming from their practical significance. To do that, the paper sets out the legal framework and requirements surrounding the submission of compliance reports. The paper then maps out the gatekeeper's compliance strategies and meters them against the benchmark of their credibility. By doing so, the paper considers a nuanced perspective of the procedural yardstick the enforcer should apply in its future enforcement action.

KEYWORDS: Digital Markets Act; Compliance Reports; Core Platform Services; Gatekeepers; Digital Regulation; Deterrence; Cooperation; Enforcement; European Commission; Digital Platforms

* Lecturer in Competition Law at University Villanueva. Email: riberamartinezalba@gmail.com. According to the ASCOLA Declaration of Ethics, the author has nothing to disclose.

[1] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ L 265, 12.10.2022.

[2] Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012.

§1.01. Introduction

The Digital Markets Act (DMA) pivots between deterrence- and cooperative-driven provisions seeking to disintermediate the magnetic power of the regulation's targets (gatekeepers) acting as private rule-makers upon their own digital ecosystems.[3] Addressing low rates of contestability and fairness within the markets they operate in is key to understanding how (and where) the regulation's mandates kick in.[4] In parallel, the DMA declares that these provisions must meet the standard of effective enforcement.[5]

However, both those statements crystallise in the real world through four different ways. First, via the *de facto* transformation of the gatekeeper's business models. Gatekeepers alter their terms and conditions considering the regulatory constraints before them. Despite the fact that the DMA's deadline for compliance for those designated gatekeepers in September 2023 was set out in March 2024, nothing stopped them from altering their operational conditions prior to the regulatory deadline.[6] Alternatively, it may well be the case that their business models already converge with the regulatory reality and, as such, no technical implementation may be warranted from their side. Second, through the disclosure of the technical solutions as enshrined in Article 11 DMA. Gatekeepers produce compliance reports (and submit them to the European Commission) amid this regulatory space. Third, by submitting audits relating to the processing of their data, following the transparency-inspired mandate under Article 15 DMA. Fourth, by instituting a compliance function within the gatekeeper's organisational structure, independent from its operational functions. Article 28 DMA requires gatekeepers to self-assess their conduct and decision-making via an in-house independent monitoring function.

---

[3] This is particularly clear when one reads DMA, *supra* n. 1, at Recitals 3, 4 and 6.

[4] The regulation sets out both contestability and fairness as their main goals as defined in DMA, *supra* n. 1, at Recitals 33 and 34 as well as Article 1(1). Their application into reality is, however, somewhat more obscure, see an in-depth analysis in Alba Ribera Martínez, *The DMA's Ithaca: Contestable and Fair Markets*, 46 World Competition 429 (2023).

[5] DMA *supra* n. 1, at Article 8(1).

[6] In fact, some of the proposed implementation stems from changes to their business models already proposed prior to the compliance deadline, see *Apple announces changes to iOS, Safari, and the App Store in the European Union*, Apple's Newsroom (25 January 2024), https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/; and *Facebook and Instagram to Offer Subscription for No Ads in Europe*, Meta Newsroom (30 October 2023), https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/.

All these enforcement actions boil down to one concept alone: that of credibility.[7] Compliance with the DMA cannot be rendered effective if the enforcer does not believe in the gatekeeper's informational disclosures, both as persuasion instruments falling in the scope of a narrative as well as means to uncovering the market reality and the impending issues surrounding them. In other words, the EC cannot place effective enforcement at a threshold so low that gatekeepers can fundamentally alter its interpretation for their own sake. The paper explores how credible the gatekeeper's compliance reports result in the face of the legal requirements of Article 11 DMA by assessing the documentation submitted by the gatekeepers in compliance with the obligation.

As of March 2024, the six designated gatekeepers in September 2023 (Alphabet, Apple, Amazon, ByteDance, Meta and Microsoft)[8] presented their first compliance reports to the European Commission.[9] Two sets of reports were produced. On one side, the targets of

[7] For the different aspects of credibility, see Julian Simon-Kerr, *Law's Credibility Problem*, 98 Washington Law Review 179 (2023). On the particular aspect of the DMA's credibility, see Anna Tzanaki and Julian Nowag, *The Institutional Framework of the DMA: From Hybrid to Mature?* (forthcoming).

[8] The European Commission designated these undertakings as gatekeepers in several decisions, see Commission Decision of 5 September 2023 designating Alphabet as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (notified under document C(2023) 6101), OJ C 549, 27.10.2023; Commission Decision of 5 September 2023 designating Amazon as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (notified under document C(2023) 6104), OJ C 905, 15.11.2023; Commission Decision of 5 September 2023 designating Apple as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (notified under document C(2023) 6100), OJ C 548, 27.10.2023; Commission Decision of 5 September 2023 designating ByteDance as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (notified under document C(2023) 6102), OJ C 552, 27.10.2023; Commission Decision of 5 September 2023 designating Meta as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (notified under document C(2023) 6105); and Commission Decision of 5 September 2023 designating Microsoft as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (notified under document C(2023) 6106), OJ C 551, 27.10.2023. After March 2024, the European Commission designated one additional gatekeeper (Booking.com), see Directorate-General for Competition and Directorate-General for Communications Network, Content and Technology, *Commission designates Booking as a gatekeeper and opens a market investigation into X* (13 May 2024), https://digital-markets-act.ec.europa.eu/commission-designates-booking-gatekeeper-and-opens-market-investigation-x-2024-05-13_en.

[9] See non-confidential versions of the compliance reports in Alphabet, *EU Digital Markets Act (EU DMA) Compliance Report Non-Confidential Summary* (7 March 2024), https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-bb_2023-9-6_2024-3-6_en_v1.pdf; Amazon, *Public Digital Markets Act Compliance Report* (7 March 2024), https://assets.aboutamazon.com/a8/33/e931dab5407bae69a8f21b31d2ad/amazon-dma-compliance-report.pdf; Apple, *Apple's Non-Confidential Summary of DMA Compliance Report* (7 March 2024), https://www.apple.com/legal/dma/dma-ncs.pdf; ByteDance, *Compliance Report (Non-confidential Version) under Article 11 of Regulation (EU) 2022/1925 of the European Parliament and of the Council (Digital Markets Act ("DMA"))* (7 March 2024), https://sf16-va.tiktokcdn.com/obj/eden-

the regulation submitted an exhaustive (and confidential) version of those reports to the European Commission, with no further circulation amongst stakeholders.[10] On the other side, the gatekeepers published non-confidential versions of the compliance reports. The analysis performed by the paper builds on the documentation belonging to this last group. Those public versions of the compliance reports present the main highlights of the undertaking's compliance with the DMA. In turn, the gatekeepers also submitted their audits on the consumer profiling they perform on their end users as enshrined in Article 15 DMA.[11] Since the nature of these audits is loosely related to the DMA's regulatory obligations contained in Articles 5 to 7, the paper does not incorporate them into its analysis. In a similar vein, due to the lack of information available, the paper does not engage in the discussion of how gatekeepers have structured their in-house DMA-driven compliance functions.

Instead, the paper depicts the road to compliance into two different sections: the intersections leading to the desired application of the DMA's provisions and the actual implementation of technical solutions. Section §1.02 points out the EC's expansion of the terms of Article 11 DMA. By doing this, the paper underlines three distinct conclusions that inadvertently permeate the compliance reports. First, the compliance reports' non-confidential versions obscure most of the under-the-hood transformations that the

va2/uhkklyeh7othpu/Bytedance%20DMA%20Compliance%20Report%20Public%20Overview.pdf; Meta, *Meta's Compliance with the Digital Markets Act: Non-Confidential Public Summary of Meta's Compliance Report* (6 March 2024), https://scontent.fmad17-1.fna.fbcdn.net/v/t39.8562-6/431009250_1846639239090452_3219463139934460359_n.pdf?_nc_cat=107&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=4TetBWnrrmEQ7kNvgFFP1PE&_nc_ht=scontent.fmad17-1.fna&oh=00_AYDxIeJd7POFMuOd3fflTyM8s5lnJpRDlnUlBV6bW_xZnQ&oe=66BA6613; and Microsoft, *Microsoft's Compliance with the DMA* (7 March 2024), https://www.microsoft.com/en-us/legal/compliance/dmacompliance.

[10] It is true, however, that some of the parts of those confidential reports correspond to previous engagements of the gatekeepers vis-à-vis stakeholders in non-public workshops where some technical implementation of the regulation was discussed.

[11] Those are available in Alphabet, *Public overview of Article 15 EU Digital Markets Act (EU DMA) report* (7 March 2024), https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-aa_2024-1-1_2024-1-1_en_GB_v1.pdf; Amazon's compliance report *supra* n. 9, at 31; Apple, *Personal Data Use for Personalized User Experiences* (March 2024), https://www.apple.com/legal/privacy/en-ww/personalized-user-experiences/; ByteDance, *Report under Article 15 of Regulation (EU) 2022/1925 of the European Parliament and of the Council (Digital Markets Act)* (26 March 2024), https://sf16-va.tiktokcdn.com/obj/eden-va2/uhkklyeh7othpu/ByteDance%20Consumer%20Profiling%20Techniques%20Public%20Overview.pdf ; Meta, *Meta's Consumer Profiling Techniques Digital Markets Act: Non-Confidential Public Overview* (6 March 2024), https://scontent.fmad17-1.fna.fbcdn.net/v/t39.8562-6/430986649_1128883765218601_1702445800238123680_n.pdf?_nc_cat=110&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=fp3reJnjrk8Q7kNvgFGwUDH&_nc_ht=scontent.fmad17-1.fna&oh=00_AYC8jkKdxxVMPK89__4ooeEVWdBpLmNIkzfZsEbA_PRoag&oe=66BA5E01; and Microsoft's compliance report *supra* n. 9.

regulation mandates vis-à-vis business users. Second, the regulation expands and shrinks depending on the captured services via the designation. This tenet of the regulation ignites the gatekeeper's tentative interpretation of the DMA, which is comprised not only of how they intend to comply with the substantive provisions under Articles 5 to 7 DMA but also of whether they can singlehandedly sidestep its application. Section §1.02.A presents the argument by correlating the DMA's scope of application and the gatekeeper's interpretation of that same subject. Third, as a result of both conclusions, compliance reports and their effectiveness in rendering useful for the enforcer rely on credibility. By this token, the paper reveals that effective DMA enforcement must be preceded by the EC's strict scrutiny of these aspects of the compliance reports.

Furthermore, Section §1.03 pierces the bubble of the first wave of compliance reports. By taking inspiration from the concept of credibility as a means of presenting plausible compliance solutions, the paper sets out the degree of transformation the DMA has brought to digital markets. Notwithstanding the moderate shift in gatekeeper attitudes towards altering their services, the paper presents, in parallel, the differences in each one of their compliance strategies and benchmarks them against the threshold of credibility.

In short, the paper puts into question the credibility of the compliance reports by assessing their practical implications. DMA effective enforcement will be as feasible as the enforcer is capable to address those shortcomings via its enforcement action.

§1.02. Compliance reports and their legal prominence in the Digital Markets Act

Compliance reports describe the gatekeeper's implementation of Articles 5 to 7 DMA into their business models. Once the undertaking is designated a gatekeeper via a designation decision, it must come up with those solutions in the short time span of six months.[12] This is the compliance deadline. In practical terms, the first six undertakings designated as gatekeepers had to comply with the DMA's provisions (except for a few exceptions) as of March 2024.[13] On the 7th of March, those gatekeepers submitted their confidential compliance reports to the European Commission whilst they also made them readily available via their websites. On that same date during subsequent years, gatekeepers will update their compliance reports to the changing economic reality.

Article 11 DMA establishes those reports must describe implementation measures in detail and transparently.[14] Gatekeepers do not simply engage in a one-off (or iterative) relationship with the European Commission.[15] Other stakeholders to the market, such as business users and third parties, are also called to gauge the gatekeeper's DMA implementation. Due to that reason, the gatekeepers shall design their compliance reports (even in their publicly available non-confidential versions) so that these agents may provide the European Commission with valuable feedback relating to any of their shortcomings.[16]

The European Commission's first enforcement actions pivot around the information catered by the gatekeepers via these compliance reports.[17] It is, therefore, surprising that they were not included in the DMA's initial institutional design, as proposed by the EC

[12] The six-month period is predetermined by DMA *supra* n. 1, at Articles 3(10) and 11(1).
[13] The twenty-core platform services designated by the European Commission had to meet this deadline, but Booking.com's compliance deadline is set for 13 November 2024 and Apple's iPadOS on 29 October 2024.
[14] Those requirements of transparency stem from the law, as reiterated by Antoine Babinet and Katarzyna Sadrak, *DMA Enforcement: Setting the Scene for Effective Compliance* (18 December 2023), https://eulawlive.com/competition-corner/op-ed-dma-enforcement-setting-the-scene-for-effective-compliance-by-antoine-babinet-and-katarzyna-sadrak/; and Alexandre de Streel, Marc Bourreau, Richard Feasey, Amelia Fletcher, Jan Krämer and Giorgio Monti, *Implementing the DMA: Substantive and Procedural Principles*, Centre on Regulation in Europe (2024).
[15] On the multi-dimensionality of iterations subsequent to the DMA's enforcement and implementation, find de Streel, Bourreau, Feasey, Fletcher, Krämer and Monti *supra* n. 14, at 93-95; and Alba Ribera Martínez, *Rocking the Contestability and Fairness Foundations: Multi-Level Governance and Trust Regulations for Futureproofing the DMA's Effectiveness*, European Yearbook of International Economic Law 1 (2023).
[16] This justification is illustrated by Alberto Bacchiega and Thomas Tombal, *Agency Insights: The first steps of the DMA adventure*, 12 Journal of Antitrust Enforcement 189 (2024).
[17] Bacchiega and Tombal *supra* n. 16, at 192-193.

in its original draft on December 2020.[18] The European Parliament's intervention in the co-legislative process introduced this aspect of the regulation, aimed at narrowing down the information asymmetries between the regulator and the gatekeepers.[19]

That is the reason behind the fact that the compliance reports stand as a middle-ground solution between the deterrence-based (for instance, the opening of non-compliance procedures) and self-regulation-driven design of the DMA.[20] The gatekeepers submit these reports to the European Commission as the regulation's sole enforcer. From the letter of the law, the EC is not required to react to them in any given form or shape. It cannot (or will not) endorse any of the compliance solutions the gatekeepers set forth in their compliance reports and it cannot punish any given conduct other than via the opening of a non-compliance procedure.[21] In this context, the compliance reports open the floodgates of information flows to the European Commission on the gatekeeper's configuration of their operations online, especially as intermediators for their business users to reach end users.[22]

At face value, however, the greater information available to the European Commission on the gatekeeper's way of functioning does not necessarily entail the targets cannot misrepresent their operations through their reporting obligations. In fact, there are two main ways by which the gatekeepers may undermine effectiveness: via the interpretation of the DMA's scope as a contentious issue and by obscuring most of the compliance reports' main advancements from its non-confidential version.

[18] For that version, see Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (notified under document COM(2020) 842 final), 15.12.2020.
[19] Pinar Akman, *Regulating Competition in Digital Platform Markets: A Critical Assessment of the Framework and Approach of the EU Digital Markets Act*, 1 European Law Review 85 (2022).
[20] Imelda Maher, *Regulatory design in the EU Digital Markets Act: no solo run for the European Commission*, 12 Journal of Antitrust Enforcement 273, 276-277 (2024).
[21] VP Vestager recognised that the European Commission would not endorse compliance solutions in Margrethe Vestager, *Discussion on the implementation of the Digital Markets Act* (3 March 2024, IMCO Committee at the European Parliament, Brussels). It is not extremely uncommon for enforcers to act in this way, see for previous experience, for instance, the seminal paper of Cary Coglianese and David Lazer, *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals* 37 Law & Society Review 691 (2003).
[22] On the hybrid nature of the DMA's addressing of information asymmetries, Tzanaki and Nowag *supra* n. 7.

[A] The scope of the DMA's provisions: credibility in interpretation

Not every single provision of the long list included under Articles 5 to 7 of the DMA is applicable to every single service catered by the gatekeepers.[23] The regulation's scope transforms depending on the concerned mandate. At the outset of designation, a gatekeeper cannot exist in the eyes of the regulation if it is not paired with the catering of a core platform service (CPS). In fact, the definition of a gatekeeper under Article 3(1) requires the undertaking's provision of a core platform service as a pre-condition to become one of the regulation's addressees.[24] In turn, Article 2 DMA defines the gatekeeper's services as CPSs if they fall under any of the categories included in the regulation. Bearing in mind the legal framework, designation operates to set apart these services as targets to the regulation.

Once designation is complete, one must turn to the substantive provisions for some guidance in unearthing the regulation's scope of application. The mandates engrained under Articles 5 to 7 DMA can be directly attributed to one of two characteristics. Either the provision's effectiveness is concomitant with its scope, or it is not. On one side, some of the mandates apply to every single CPS category, since their scope is not ancillary to its effectiveness. For instance, Article 5(6) prohibits the restrictions imposed by the gatekeepers on business and end users hindering their capacity to raise any issue of non-compliance with any relevant public authority related to the gatekeeper's practices. In turn, other obligations only apply to certain CPS categories, and that determination is particularly relevant for metering compliance. As a matter of example, Article 5(2) prohibits the cross-using of personal data across different CPSs. If one feature of the service falls inside or outside a particular CPS's scope, this finding is not completely frivolous or non-consequential for the regulation's application. Instead, it renders a decisive factor in metering the gatekeeper's compliance with the provision.

[23] Table 2 under the Annex explains the relationships between each CPS and the scope of application of each provision.

[24] As explored by Pablo Solano Díaz, *Of Core Platform Services, Fairness and Contestability – Competition law through the Hall of Mirrors* (30 November 2023), https://eulawlive.com/competition-corner/op-ed-of-core-platform-services-fairness-and-contestability-competition-law-through-the-hall-of-mirrors-by-pablo-solano-diaz/; and in more detail by Friso Bostoen and Giorgio Monti, *The Rhyme and Reason of Gatekeeper Designation under the Digital Markets Act* (forthcoming); and Alba Ribera Martínez, *The Requisite Legal Standard of the Digital Markets Act's Designation Process*, Journal of Competition Law & Economics (forthcoming).

Against this background, the European Commission has not explicitly (nor publicly) defined each provision's scope. No single enforcement tool embedded in the regulation requires it to. Aside from that, based on the six designated gatekeepers in September 2023 relating to the twenty-two captured CPSs, in the hypothetical case that the EC was to perform the exercise, it would have to communicate its interpretation regarding 484 combinations of each provision per CPS. Therefore, the reversal of the burden of intervention against the gatekeeper when submitting its compliance report already encompasses this exercise.[25] The gatekeeper is not strictly tied to any given interpretation of a provision's scope, but it must, in fact, consider it as a pre-condition to determining whether any substantial change of its business models is warranted on its side.

By this token, one could expect two consequences to crystallise into reality. Either the gatekeeper interprets that a provision it should comply with does not apply to a particular CPS or the gatekeeper implements technical implementation for a CPS where compliance is not legally mandatory. Building upon an interpretation of each provision's scope of application, only some of the gatekeepers have tested out the limitations of the compliance reports in this regard.[26]

Stemming from the 484 possible combinations of compliance resulting from the first wave of reports, most of the undertakings stood within the limits of a reasonable interpretation of the DMA. In contrast, Alphabet and ByteDance's submissions rendered the most problematic.[27] From all the existing combinations, approximately 5% of the gatekeeper's interpretations over the DMA's scope of application contradicted the terms of the regulation.[28] For instance, ByteDance argues it is not compelled to comply with the terms of Article 6(2) DMA, mandating gatekeepers to silo the data their business users generate within their CPSs from the data they use to compete with them. The undertaking's interpretation is striking since Article 6(2) is transversally applicable to all

[25] The concept of the reversal of the burden of intervention was first addressed by Pablo Ibáñez Colomo, *Draft Digital Markets Act: A Legal and Institutional Analysis*, 12 Journal of European Competition Law & Practice 561 (2021).
[26] Under the Annex to the paper, Table 2 sets out each of the provision's scope of application, deriving from an interpretation of each mandate and their corresponding recitals. The table was originally prepared by the author in a forthcoming paper, see Giuseppe Colangelo and Alba Ribera Martínez, *The Secret (Metrics) of DMA Success* (forthcoming).
[27] Table 1 included under the Annex plots the 484 combinations by spotting the divergences between the expected interpretation, as stemming from the letter of the law, and the compliance report's proposed application of the DMA's provisions.
[28] The percentage corresponds to 25 instances where the gatekeeper's interpretation is deemed problematic as shown in Table 1, out of the 484 possible combinations.

categories of CPSs, and the characterisation as a gatekeeper implies that the undertaking bears a dual role in providing a gateway for business users to reach end users. Despite the clear relationship, ByteDance defended the provision does not apply to it since it does not hold a dual role as envisaged by the mandate.[29]

In a similar vein, Alphabet, for example, meters compliance with Article 6(8) DMA quite narrowly. The obligation allows business users to access performance measuring tools and the data necessary to carry out verification to assess the accomplishments of their ads within the gatekeeper's CPSs. Similarly to Article 6(2) DMA, the provision does not simply apply to a particular CPS category. Rather, it applies to all twelve categories included under Article 2 DMA. However, Alphabet does not share that same interpretation and declares that it only applies to online advertising services. On its compliance report, it only proposed technical implementation for its online advertising service designated by the EC, whereas for the other seven CPSs that remain captured by the DMA (Google Search, YouTube, Google Android, Google Chrome, Google Play, Google Shopping and Google Maps) it generally observed the provision was not applicable.[30] In practical terms, Alphabet's interpretation implicitly translates into a clear conclusion: the ads displayed on any of those services do not remain captured by the provision. Alphabet's interpretation follows, in fact, the EC's own designation decision, since it repeatedly established that ads displayed on the rest of CPSs should be understood as falling within the scope of the online advertising services, and not to those CPSs.[31] Every single piece of data is channelled through data aggregation at the technical level of Alphabet's online advertising services. Notwithstanding, the provision is not exclusively directed at advertisers and publishers, but also at third parties authorised by them which will retrieve data from different sources so to paint a more complete picture of their ads' performance and valuation. Therefore, the gatekeeper's interpretation shifts compliance away from any of the third parties relying on Alphabet's CPSs other than its advertising services.

Even though both examples seem trivial and unimportant before the high task of seeking effective DMA enforcement, they demonstrate both the technical complexity of correctly interpreting the regulation as well as the gaping holes the gatekeepers may take advantage

[29] ByteDance's compliance report *supra* n. 9, at 22.
[30] Alphabet's compliance report *supra* n. 9, at 99-101, 122, 134, 143, 166, 192 and 204.
[31] Alphabet's designation decision *supra* n. 8, at paras 38, 59, 78, 96 and 115.

of by slowly sidestepping the DMA's application. If a gatekeeper fights the scope of application of a provision, then the burden reverts to the EC to prove the undertaking wrong so that the burden of proposing new compliance solutions shifts back to the gatekeeper. In turn, the gatekeeper will not deliver the renewed technical implementation within the expected compliance deadline nor in the quickest possible manner, contrary to the regulation's desire to keep fast paced in its enforcement.

[B] A faithful comprehensive and meaningful picture of the compliance report

The DMA derives its legitimacy and its effectiveness not from its direct outputs, but from the prospects it generates for third parties.[32] Third parties, distinct from the gatekeepers, hold instrumental to the DMA's effective enforcement.[33] For instance, business users must seize the opportunities to compete on the merits with the gatekeepers when their capacity to access the data they generate on CPSs is readily available to them via Article 6(10).

Third parties will be, thus, kept informed about what avenues and business opportunities they may grasp via the compliance reports, namely via the non-confidential summary the gatekeeper publishes on its website.[34] Prior to the initial compliance deadline, the European Commission issued an implementing act fleshing out the requirements those compliance reports should meet.[35] Section 4 of that implementing act requires the non-confidential summary of the compliance report to provide meaningful input to the Commission on the undertaking's compliance with its obligations under the DMA.

[32] For the aspects of input, output and throughput legitimacy related to the DMA, see Alba Ribera Martínez, *The Steering of End-User Behaviour in the Digital Markets Act: The Intrinsic Value of Trust for Governance*, 9 North East Law Review 8, 9 (2022).
[33] Olivier Guersent, *Annual CRA Brussels Conference* (6 December 2023, Brussels).
[34] DMA *supra* n. 1, at Article 11(2).
[35] *Template Form for Reporting Pursuant to Article 11 of Regulation (EU) 2022/1925 (Digital Markets Act) (Compliance Report)* (9 October 2023), https://digital-markets-act.ec.europa.eu/document/download/904debdf-2eb3-469a-8bbc-e62e5e356fb1_en?filename=Article%2011%20DMA%20-%20Compliance%20Report%20Template%20Form.pdf. Although the DMA *supra* n. 1, at Article 46(1)(f) provides for the possibility of the EC to adopt these implementing provisions, this implementing act did not follow the mandatory procedure established in the regulation for that purpose, as highlighted in Dirk Auer and Lazar Radic, *Enforcing the DMA is Easier Said Than Done: Evidence From the Commission's Draft Template for DMA Compliance Reports* (5 July 2023), https://truthonthemarket.com/2023/07/05/enforcing-the-dma-is-easier-said-than-done-evidence-from-the-commissions-draft-template-for-dma-compliance-reports/; and Alba Ribera Martínez, *The European Commission's (Draft) Template for DMA Compliance Reports: Sailing Through Rough Seas* (8 June 2023), https://competitionlawblog.kluwercompetitionlaw.com/2023/06/08/the-european-commissions-draft-template-for-dma-compliance-reports-sailing-through-rough-seas/.

Compliance reports (even in their non-confidential versions) must comprise a faithful comprehensive and meaningful picture of their content.

Therefore, the European Commission, as the sole enforcer and main interpreter of the regulation, places a high burden of intervention on the gatekeeper to document its technical implementation of the regulatory instrument. It must extensively communicate its compliance solutions to the EC via its confidential report. In turn, the non-confidential version of those reports must be consequential and purposeful for third parties, i.e., meaningful. These compliance reports signal the venues for business opportunities on the side of the gatekeeper's competitors.

One would have expected, thus, those non-confidential summaries to include every single implementation of those provisions which apply to each of the gatekeeper's CPSs. This was the case for some of them. For instance, Alphabet, ByteDance, and Microsoft presented comprehensive accounts of their technical implementation of the DMA dissected per each provision and CPS.[36] Other gatekeepers obscured their compliance reporting by interpreting the feature of 'meaningfulness' in a restrictive way. For example, Amazon included in its compliance report seven of its technical solutions for its Amazon Advertising CPS, whereas it did not include compliance solutions for seven of the provisions that were applicable to it.[37] In a similar vein, Apple's compliance report contains four compliance proposals for its web browser Safari CPS as opposed to the rest of the six provisions which were equally applicable to the CPS in terms of the scope of their application, which remained unaddressed.[38]

Despite the EC's unwillingness to provide intensely prescriptive instructions on the compliance reporting obligations of gatekeepers, some of the regulation's addressees displayed broad discretion in interpreting what a meaningful compliance report should look like. Reservations about the compliance report's credibility arise in this context as they did with respect to the interpretation of the scope of application of each provision.[39]

---

[36] In fact, Template Form for Reporting Pursuant to Article 11 of Regulation (EU) 2022/1925 (Digital Markets Act) (Compliance Report) *supra* n. 35, at Section 4.b) and c) requires the gatekeepers to submit a compliance report with the same format as the template and to separate the technical implementation of the regulation per each core platform service.
[37] Amazon's compliance report *supra* n. 9, at 5-9, 19, 21-26 and 30.
[38] Apple's compliance report *supra* n. 9, at 4 and 5.
[39] This aspect was already raised, in economic terms, by Amelia Fletcher, Jacques Crémer, Paul Heidhues, Gene Kimmelman, Giorgio Monti, Rupprecht Podszun, Monika Schnitzer, Fiona Scott Morton and

Likewise, the European Commission as the sole enforcer cannot do much other than informally pressure the regulation's addressees. Triggering a non-compliance procedure on these grounds would hardly be sustained in the law. Article 29 DMA categorises infringements to the DMA as those operating under a violation of Articles 5, 6 and 7 of the regulation. As opposed to the potential risk of undermining the regulation's effectiveness, falling within the remit of Article 13, the incomplete submission of non-confidential reports (based on Article 11 DMA) misses the mark of sustaining a standalone infringement whilst substantially undermining the DMA's efficacy with respect to third parties.[40]

§1.03. The first wave of compliance reports: the gatekeeper's compliance strategies

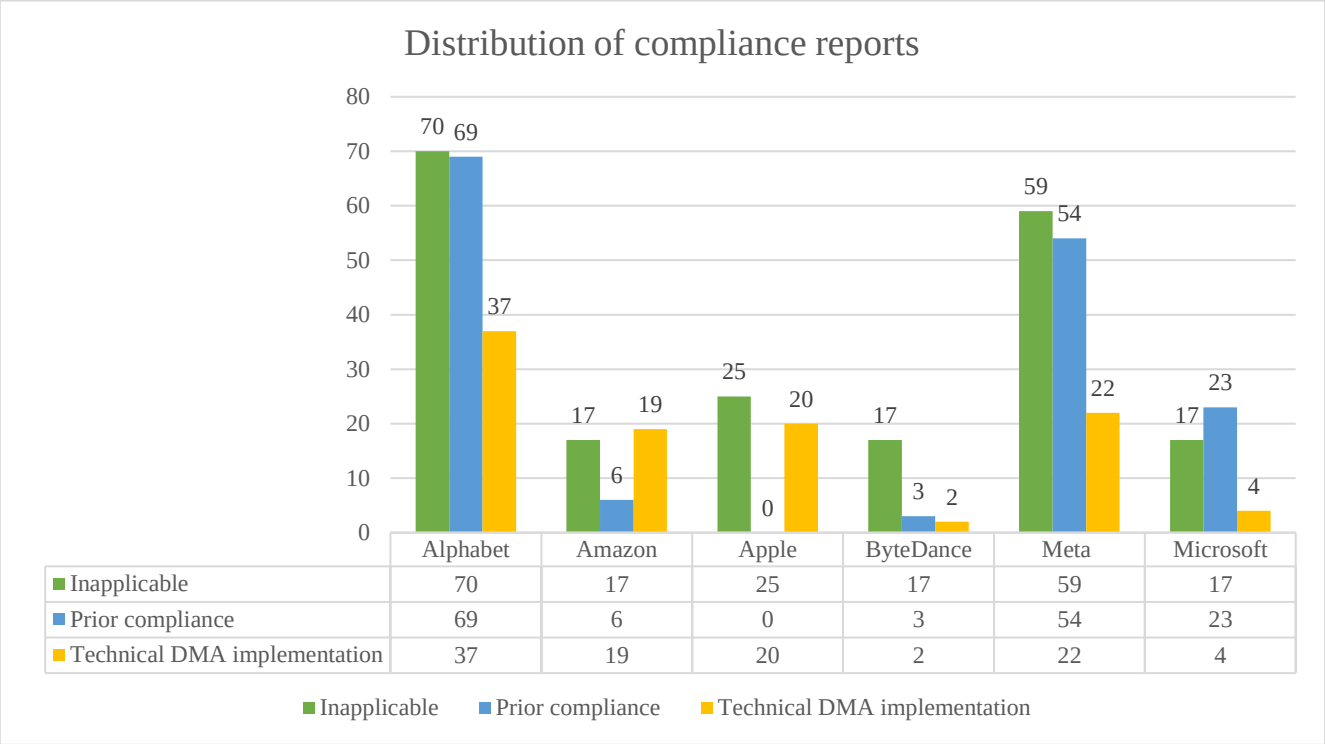
Six reports represent the first wave of DMA compliance. They are the first snapshots to the transformation in digital business models that the regulation introduces. In the same spirit of exercising a wide margin of discretion in interpreting the regulation's provisions, gatekeepers have not only mapped out the provisions which apply to each of their CPSs depending on their scope of application. Gatekeepers have further categorised implementation with the DMA into two temporal dimensions: the past and the future.

Aside from those provisions which are not directly applicable in terms of scope, compliance entails that gatekeepers must identify the areas of improvement (and mandatory transformation) correlated to the regulation's provisions. Even though the DMA establishes prescriptive and proscriptive mandates to steer digital competitive dynamics in one direction or another, gatekeepers defend that, in most cases, the current configuration of their business models already adapts to the regulation's requirements. In other words, their past operations stay in compliance with the regulation, as opposed to those changes required by the DMA's mandates, i.e., the present. Figure 1 maps out how the gatekeepers categorise provisions in this fashion, as stemming from their compliance reports:

Alexandre de Streel, *The Effective Use of Economics in the EU Digital Markets Act,* 20 Journal of Competition Law & Economics 1, 15 (2024).

[40] The DMA does not even provide a particular sanction for these types of cases under DMA *supra* n. 1, at Article 30(3), corresponding to those infringements imposing fines not exceeding 1% of their total worldwide turnover in the preceding financial year.

Figure 1. Distribution of compliance reports.



From Figure 1, four types of compliance strategies arise from the gatekeeper's reporting obligations. First, a focus on the submission of evidence and arguments advocating in favour of minimal compliance with the DMA. In other words, the gatekeepers focus their efforts on the few instances of technical implementation of the DMA, whereas they grant no particular attention to the bulk of the provisions applicable to them. Either they consider that they are inapplicable in terms of scope, or they defend that their business model already stood in compliance with the regulation. Alphabet, Meta and Microsoft stand as the clearest examples of this first group.[41]

However, the reasoning that goes into this first group of compliance strategies takes different forms. The recurring reasoning they put forward is that they have themselves verified they do not perform the captured conduct by the DMA. For instance, Meta defends the terms of its Facebook Marketplace service do not restrict users from offering their products or services on other platforms at whichever conditions they choose. Thus, Meta interprets it as already complying with Article 5(3), and no further action is

[41] If one adds up inapplicability with prior compliance and compares it to technical DMA implementation, Alphabet's compliance strategy focuses on 27% of the provisions contained in the DMA, Meta stands at 20% and Microsoft at 10%.

warranted.[42] It is straightforward enough. More sophisticated arguments go into sustaining prior compliance with the DMA. For instance, Alphabet holds its Google Android operating system already complies with the vertical interoperability mandate embedded in Article 6(7). The gatekeeper establishes it permits third-party app and hardware developers to access and interoperate with its own operating system in the same way as Google's first-party apps and hardware.[43] Business users voiced their concern contesting the validity (and truthfulness) of this interpretation since third-party apps do not enjoy the pre-installation privileges of Alphabet's proprietary apps.[44] The most salient aspect of Alphabet's stance is that it seeks to exclude any regulatory scrutiny on the enforcer's side.

On the contrary, Microsoft's compliance strategy stands in stark contrast to Meta's and Alphabet's, since prior compliance with the DMA does not hinder it from proposing technical improvements to its products and services. In fact, Microsoft seizes the legal requirements as opportunities to avoid further regulatory scrutiny and introduces compliance solutions, out of precaution.[45] For instance, relating to the obligation prohibiting engrained default settings into the operating system (Article 6(3) DMA), Microsoft observes it already complies with the provision. Users can easily uninstall applications and change their default settings on Windows 10 and 11. Notwithstanding, it thoroughly reviewed its approach to what features of Windows constitute software applications and made sure that all applications on Windows 10 and 11 are uninstallable. In parallel, Microsoft ensured that for Windows devices operating in the EEA, when a user clicks on a link or file type, Windows uses the default application to open it.[46]

Common characteristics to the rest of compliance strategies cannot be identified with any other group of gatekeepers, but each of the remaining targets represents a different one. Amazon's approach towards compliance is that of demonstrating a high degree of transformation within its business model. Nonetheless, the few instances where prior compliance is asserted are those that have drawn the most attention from competition

[42] Meta's compliance report *supra* n. 9, at 51.
[43] Alphabet's compliance report *supra* n. 9, at 122.
[44] Andy Yen, *Google's DMA compliance plan is a sham* (6 June 2024), https://proton.me/blog/google-bundling-ignores-dma.
[45] Microsoft's legal representatives even recognised this compliance strategy in its *Microsoft DMA compliance workshop* (26 March 2024, 13:00-18:00), https://digital-markets-act.ec.europa.eu/events-poolpage/microsoft-dma-compliance-workshop-2024-03-26_en.
[46] Microsoft's compliance report *supra* n. 9, at 65-84.

authorities in the past. Amazon introduces substantial changes in terms of data access for both end and business users, presented in detail throughout the report.[47] In turn, however, it asserts that it already complies with the data siloing obligation under Article 6(2) after having concluded an exhaustive analysis of its internal systems.[48] This aspect of the regulation is the most controversial for the gatekeeper since it stems from previous (mainly unresolved) sanctioning proceedings triggered by the European Commission and the Italian national competition authority enquiring on the anti-competitive nature of this same conduct.[49]

Moreover, from Apple's non-confidential version of the compliance report, the gatekeeper simply does not provide sufficient insight into its interpretation of the DMA.[50] This compliance strategy does not fall short of Apple's overall dynamic understanding of how it should operate with regard to the DMA. Even though the compliance deadline was set for March 2024, Apple presents a fragmented and patchworked account of its technical solutions by constantly updating substantive parts of its technical implementation via informal channels of information.[51] By this token, the regulation's target disperses regulatory scrutiny across different sources and term of services' versions.

---

[47] Amazon's compliance report *supra* n. 9, at 4-13.

[48] *Ibid*, at 30; and *Amazon DMA compliance workshop* (20 March 2024, 13:00-18:00), https://digital-markets-act.ec.europa.eu/events-poolpage/amazon-dma-compliance-workshop-2024-03-20_en. In fact, the European Commission is enquiring on whether that conclusion is true, see *Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act* (25 March 2024), https://digital-markets-act.ec.europa.eu/commission-opens-non-compliance-investigations-against-alphabet-apple-and-meta-under-digital-markets-2024-03-25_en.

[49] *Antitrust: Commission accepts commitments by Amazon barring it from using marketplace seller data, and ensuring equal access to Buy Box and Prime* (20 December 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777; and *A528 – Italian Competition Authority: Amazon fined over € 1,128 billion for abusing its dominant position* (9 December 2021), https://en.agcm.it/en/media/press-releases/2021/12/A528.

[50] For instance, Apple's compliance report *supra* n. 9, does not include technical implementation (or any further explanation on whether it is needed) for Articles 5(5), 5(6), 5(8), 6(6), 6(10) and 6(13) with reference to its iOS CPS or Articles 5(3), 5(5), 5(8), 6(3), 6(4), 6(5), 6(6), 6(12) and 6(13) relating to its App Store.

[51] Most of these updates happen via its section of developer documentation where compliance shapeshifts across time, see, for instance, Ivan Mehta, *Apple changes App Store rules to allow retro game emulators globally* (5 April 2024, 11:46), https://techcrunch.com/2024/04/05/apple-changes-app-store-rules-to-allow-retro-game-emulators-globally/; Natasha Lomas, *Apple ads more carve-outs to its EU core tech fee after criticism from devs* (2 May 2024, (8:00), https://techcrunch.com/2024/05/02/apple-adds-more-carve-outs-to-its-eu-core-tech-fee-after-criticism-from-devs/; and Natasha Lomas, *Apple revises DMA compliance for App Store link-outs, applying fewer restrictions and a new fee structure* (8 August 2024, 9:00), https://techcrunch.com/2024/08/08/apple-revises-dma-compliance-for-app-store-link-outs-applying-fewer-restrictions-and-a-new-fee-structure/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALkDu5ZHrm-B1ao5Kn4I00urtwTeCI_1MERmAvHsNR59fgELLw2kX1EX9NXg0cbGKNHtlnkHtu4yQatsrdQFqAJC

Finally, ByteDance presents quite a convoluted compliance strategy, mirroring Microsoft's approach in the inverse. Instead of directly sustaining that its TikTok service already complies with the regulation in some respects, ByteDance sustains most of the provisions do not apply to it for different reasons. For instance, it considers that Article 6(12) requiring gatekeepers to provide FRAND-like access to their social networking services does not apply to it in terms of scope. At face value, the assertion seems hard to believe, since TikTok was designated as a social networking service by the European Commission.[52] In any case, and out of precaution, ByteDance goes into greater detail to demonstrate that the terms and conditions in which access is rendered to business users meet the provision's standards.[53] ByteDance masks its compliance intentions via the transformation of its platform with the inclusion of additional explanations of why those changes are not warranted. In reality, however, its compliance report only contains two instances where substantial modifications have been made to its overall business strategy and platform design.[54] In principle, this is nothing to be ashamed of and does not, *per se*, undermine effectiveness. If the DMA simply does not apply to a target but for a few obligations, the compliance report should operate more to clarify the scope and weight of technical implementation than to contradict its own terms.

Within this scale of different compliance strategies, some of them demonstrate a greater reluctance to substantially engage with the regulation whereas others prove the gatekeepers to be particularly responsive to the regulation's demands. In any case, each of the approaches enshrines the need for the European Commission to take issue with the compliance reports not only regarding their substance but also relating to their design as presented by the gatekeepers. Credibility stands as the means to take stock of all their aspects by assigning a different rate of engagement with the DMA's spirit to each gatekeeper, depending on their interpretation of the regulatory setting.

bUmFUJSHfILYi_sH4VLdugLxUOafgSSrxuOrFXPdrvObrN6mVUvXS7tzLEgkN2q6PX6LxZFQqMyRIwhiK9l8.

[52] Despite that ByteDance notified to the EC that it should be categorised as a video-sharing platform, the EC determined it must be understood within the wider category of social networking, see ByteDance's designation decision *supra* n. 8, at paras 26-66.

[53] ByteDance compliance report *supra* n. 9, at 48-50.

[54] The gatekeeper proposed dedicated compliance solutions with respect to Articles 5(2) and 6(9) in isolation, ByteDance compliance report *supra* n. 9, at 13-19 and 25-30.

§1.04. How credible are the compliance reports?

The DMA is premised on the existence of a lack of trust of enforcers vis-à-vis the gatekeepers. These undertakings emerge with considerable economic power leading to serious imbalances in bargaining power leading to unfair practices and conditions for CPS business users and users. In turn, those conditions operate to the detriment of prices, quality, fair competition, choice and innovation. In sum, these market processes are incapable of ensuring fair economic outcomes.[55] Against this framework, the EU legislature has chosen to introduce *ex ante* rules that reverse the burden of intervention upon the gatekeeper to submit compliance reports. The EC, therefore, must first assess the question of credibility when confronting the analysis of these reports.

But what is credibility? Definitions of credibility focus on the capacity of something or someone to be believed or trusted.[56] Belief and trust share their common linguistical roots in the pursuit of truth and the reliance one holds for another's veracity. In turn, the association of both concepts with persuasiveness renders in a quasi-automatic manner. Credibility has the capacity to turn into an attribute of a subject (belief/trust) and/or of a particular narrative (persuasiveness).[57]

Going back to the DMA's compliance reports, the question of credibility permeates the three different problems delineated in the paper. The main dilemma arising from them is that persuasiveness relies on context and intuition, and most of the conclusions highlighted throughout the paper are quite counter-intuitive to grasp. Why would a gatekeeper defend that a particular provision does not apply to a CPS because it remains outside its scope of application? Or how is a particular compliance strategy more credible as opposed to the other? It all boils down to the obscured part of the DMA's enforcement.

The EC has implicitly decided to remain less prescriptive in terms of its enforcement actions and, thus, not channel its resources to setting out in black and white what the gatekeepers must do procedurally. And that opens the door for the three vectors impinging on the gatekeeper's credibility from the outset. First, in an inward-looking fashion,

[55] DMA *supra* n. 1, at Recitals 3-5. In fact, the General Court also mentioned these aspects as the regulation's main characteristics, see Case T-1077/23, *Bytedance v Commission*, 17.7.2024, ECLI:EU:T:2024:478.
[56] The common characteristic is extracted from three different dictionaries, namely Cambridge, Merriam-Webster and Collins Dictionary.
[57] Simon-Kerr *supra* n. 7, at 194.

gatekeepers bear the possibility of interpreting the scope of application of the DMA's provisions in the widest possible way. That same possibility projects in the opposite direction. This aspect touches upon credibility in its most primal state. If a gatekeeper does not correctly identify the provisions applicable to it, then the enforcer should, at least, question the gatekeeper's propensity for truth across the compliance report on its own merits. Due to its proximity to the application of the substantive provisions, the EC is, in this way, most apt to intervene to avoid the DMA being undermined in its effectiveness. In theory, at least, the EC could individually defend and pressure the gatekeeper to comply with a provision which it has 'declared' inapplicable via the opening of a non-compliance procedure since it can touch upon more than one provision.[58]

Second, looking outwards and in terms of the gatekeeper's projections to third parties, credibility may also be put into question in the absence of information deriving from the gatekeeper's non-confidential versions of their reports. The enforcer will likely draw inferences and make predictions in the face of uncertainty once confronted with this situation. If a report is not sufficiently comprehensive so that business users may seize the opportunities it presents, then its capacity to be worthy of belief decreases in the eye of the enforcer. Ironically, however, there is no credible threat that the EC may set forth so as to disincentivise the motion as deriving from the letter of the law. As opposed to the previous tenet, the EC cannot trigger an individual action to sanction the gatekeeper for an infringement of the terms of Article 11 DMA.

And finally, it all boils down to the compliance strategies each of the gatekeepers present to the enforcer via their reporting obligations. On top of the previous criticisms, credibility in its manifestation as persuasiveness is clearly disputed at the outset. This is the point where the enforcer must intuitively assess whether the narrative presented by the gatekeeper matches up to the reality of the market or whether it is obscured by that same narrative. In other words, the European Commission must consider whether the compliance strategy presented by the gatekeeper is factually, legally and contextually

[58] For instance, the EC's latest decision opening a non-compliance procedure takes issue with compliance with four different provisions, see Commission decision opening a proceeding pursuant to Article 20(1) of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (notified under document C(2024) 4509), 24.06.2024.

plausible, bearing in mind the three vectors as cumulative interpretations oriented at the same goal.

§1.05. Conclusions

The DMA imposes an *ex-ante* regime on gatekeepers seeking to restore contestable and fair markets. To do that, the EU legislature chose to impose reporting obligations on gatekeepers. The first wave of compliance reports submitted by the targets of the regulation present substantive challenges for the enforcer in its monitoring position, both from the substantive and procedural viewpoints. The paper deals with the latter to contest whether those compliance reports are to be understood as entirely credible means and demonstrations of compliance.

Three aspects of the compliance reports pose significant questions about their credibility, despite (or rather, due to) their counter-intuitive nature. First, how the gatekeepers interpret the regulation's applicability. Second, the opacity of some of the non-confidential versions of those reports, available to the public. Third, the wide array of compliance strategies one can derive from the procedural design of the compliance reports. All three vectors stand before the enforcer as a preliminary analysis so as to secure whether the compliance reports meet the requirement of effective enforcement. The first and third tenets are easily capturable via a wide interpretation of the anti-circumvention clause under Article 13 DMA, whereas the second demonstrates more elusive in practice. The paper, therefore, proposes the nuance of the sociologically oriented concept of credibility to capture the three phenomena in the pursuit of factually, contextually and legally feasible compliance solutions.

Annex I: Methodology on the DMA's scope of application and compliance reports

Table 1. Projected combinations of expected interpretation of the DMA's scope of application per each CPS (plotted from 1-22 at the top of axis) against each provision (left-hand axis).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
5(2)																						
5(3)					7																	
5(4)														18								
5(5)				**5**										19								
5(6)																						
5(7)	**1**																					
5(8)														20								
5(9)																						
5(10)																						
6(2)														21								
6(3)						10																
6(4)																						
6(5)					8									22							25	
6(6)					**9**	**11**	**14**	**16**														
6(7)						12																
6(8)	2	3		6		13	15	17						23								
6(9)																						
6(10)																						
6(11)																						
6(12)			4											24								
6(13)																						
7																						

Table 1 plots the 484 combinations of proposed compliance as stemming from the compliance reports. Cells highlighted in green correspond to those applicable provisions to each CPS, whereas cells highlighted in yellow correspond to those which are not. The twenty-five (25) cells shaded in red note the divergence between those instances where the provision was applicable and the gatekeepers interpreted it was not, without further explanation to its reasons.

Methodology underlying Table 1

The scope of application per each provision applicable to each column and row derive from Table 2 below as a general matter.

Table 2. Detail of each DMA provision's scope of application.

Provision	*Scope of application*
Article 5(2): prohibition of processing and cross-using personal data across CPSs.	Wider than the CPS categories (including third-party services and the gatekeeper's proprietary services).
Article 5(3): prohibition of parity clauses.	Applicable to online intermediation services.

Article 5(4): provision on anti-steering of communications and promotions of offers to end users.	Wider than the CPS categories (focus on end users acquired via the CPS or through other channels).
Article 5(5): provision on anti-steering on services, content, subscriptions, features or items.	Applicable to software applications (i.e., apps).
Article 5(6): elimination of restrictions in raising non-compliance issues relating to the gatekeeper.	Wider than the CPS categories (relates to any practice of the gatekeeper).
Article 5(7): prohibition on tying of alternative payment services, sign-in services and default web browsers.	Wider than the CPS categories (related to the provision of identification services, web browser engines, payment services or technical services in support of payment services supported on that CPS).
Article 5(8): prohibition of conditioning the use, access or signing up to a service with a subscription service.	As wide as the CPS categories.
Article 5(9): sharing with advertisers information on price, fees paid, remuneration received by publishers and metrics.	Applicable only to online advertising services.
Article 5(10): sharing with publishers information on price, fees paid, remuneration received by publishers and metrics.	Applicable only to online advertising services.
Article 6(2): imposition of data siloing obligation on business user data generated on the CPS.	Wider than the CPS categories (data generated by business users on the CPS and on the relevant services provided together with, or in support of the relevant CPS).
Article 6(3): allowing of un-installation and prompt default selection.	Applicable only to operating systems, virtual assistants and web browsers.
Article 6(4): alternative distribution of third-party apps or app stores.	Applicable only to operating systems.
Article 6(5): prohibition of self-preferencing.	Applicable only to online intermediation services, online social networking services, video-sharing platform services, virtual assistants, and online search engines and software application stores.
Article 6(6): enabling of switching of secondary services.	Wider than the CPS categories (services accessed using the CPSs and software applications).
Article 6(7): mandate of vertical interoperability.	Wider than the CPS categories (hardware and software features accessed or controlled via the operating system or virtual assistants).
Article 6(8): access to performance tools and verification data.	As wide as the CPS categories.
Article 6(9): right of enhanced end user data portability.	As wide as the CPS categories.
Article 6(10): access to business users to the data generated on the CPS.	As wide as the CPS categories.
Article 6(11): FRAND access to search data.	Applicable only to online search engines.
Article 6(12): FRAND access to particular services.	Applicable only to online search engines, social networking services and software application stores.
Article 6(13): termination of services abiding by the principle of proportionality.	As wide as the CPS categories.

Article 7: mandate of horizontal interoperability.	Applicable only to number-independent interpersonal communication services (and potential expansion to online social networking services via the EU legislator's explicit mandate).

Furthermore, each of the core platform services numbered 1 to 22 at the top axis correspond to the following list of designated gatekeepers correlated with their corresponding as CPSs as included in the first wave of designation decisions, as shown in Table 3 below:

Table 3. List of CPSs included under Table 1 correlated with each service and the CPS category they belong to.

Number	*Core platform service*	*Type of core platform service*
1	Google Search.	Online search engine.
2	YouTube.	Video-sharing platform service.
3	Google Android.	Operating system.
4	Google Chrome.	Web browser.
5	Online advertising.	Online advertising service.
6	Google Play.	Online intermediation service.
7	Google Shopping.	Online intermediation service.
8	Google Maps.	Online intermediation service.
9	Amazon Marketplace.	Online intermediation service.
10	Amazon Advertising.	Online advertising service.
11	iOS.	Operating system.
12	App Store.	Online intermediation service.
13	Safari.	Web browser.
14	TikTok.	Online social networking service.
15	Facebook.	Online social networking service.
16	Instagram.	Online social networking service.
17	WhatsApp.	Number-independent interpersonal communication service.
18	Meta Ads.	Online advertising service.
19	Messenger.	Number-independent interpersonal communication service.
20	Marketplace.	Online intermediation service.
21	Windows Client PC OS.	Operating system.
22	LinkedIn.	Online social networking service.

Explanation of Figure 1

Figure 1 maps out the structure of the compliance reports by categorising each of the gatekeeper's statements into three different categories: 1) not applicable; 2) prior compliance; and 3) technical DMA implementation. The first category corresponds to those provisions the gatekeeper does not consider applicable to each one of the CPSs. The second category signals those instances where the target explicitly asserts the CPS already adjusts to the DMA's legal requirements. Finally, the last category accounts for those provisions which require a dedicated technical solution on the addressees' side.