The Digital Markets Act

Antitrust 2.0 for the Tech Superpowers

And Why it Could be Much Worse News for Google's Search Manipulation Practices than Many Commentators Realise

Adam Raff and Shivaun Raff
Co-founders of Foundem and SearchNeutrality.org

23 November 2022

Table of Contents

1 Introduction

The Digital Markets Act (DMA) provides regulators with enhanced enforcement powers and a fast-track process that should help to reign in the ability of digital "gatekeepers" to skew competition and/or impose unfair conditions on the businesses and consumers that use (and often depend) on their services.

In essence, the DMA recognises and seeks to address the extraordinary power that these digital gatekeepers can often wield over their essentially captive audiences, whilst not necessarily fulfilling the traditional notion of dominance. If properly enforced, compliance will require the world's tech superpowers to make unprecedented changes to their business practices, and in some cases to their business models.

The DMA is scheduled to come into force in Spring 2023[1] and is intended to address the inherent weaknesses in current EU competition regulations, which are widely viewed as too cumbersome to protect fast moving digital markets and too weak and inflexible to impose effective remedies.

A Fast Track to Enforcement

Under current EU Competition law, taking action against a company that is abusing its dominant market position requires regulators to define the market, demonstrate that the company is dominant in that market, and finally demonstrate that the practice(s) at issue have appreciably harmed (or had the potential to harm) competition and were not objectively justified.

The DMA streamlines all three of these steps by proactively defining a set of markets (the "core platform services"); establishing rules that pre-determine the broad equivalence of dominance within those markets ("gatekeeper designations"); and codifying a set of "obligations" that recognise that certain business practices should be presumed to harm competition and consumer choice when deployed by a digital gatekeeper.

Pre-Packaged Prohibition Decisions

In a sense, the DMA provides the broad equivalent of pre-packaged Prohibition Decisions for certain kinds of practices in certain kinds of digital markets, which should allow the Commission to progress rapidly to the cease-and-desist enforcement stage when digital gatekeepers fail to meet their obligations. In the process, the DMA removes the burden for regulators to demonstrate the actual or potential harm of these kinds of practices in the hands of each individual gatekeeper. And, importantly, it neutralises the ability for gatekeepers to run their often vacuous and always time-consuming efficiency or objective justification arguments.[2]

The Codification of Anti-Competitive Leveraging on Steroids

Moreover, while the DMA does aim to protect competition ("contestability") within the core platform markets, much of it is also aimed at preventing anti-competitive leveraging into adjacent markets. Certain aspects of the DMA might best be viewed as a codification of the concept of anti-competitive leveraging on steroids. For example, many of the gatekeeper obligations reflect the fact that the ability to exert power over a wide array of downstream and/or adjacent markets is often a key feature of these digital platforms.

---

[1] The European Parliament voted to adopt the DMA on 5 July. The European Council ratified this decision on 18 July, and it was published in the Official Journal in October 2022. The obligations under the DMA will become active six months after publication (April 2023), and gatekeepers will need to comply with their obligations by early 2024.

[2] See, for example, recital 10

2 Core Platform Services: Defining the Key Digital Markets

The DMA defines and targets ten broad categories of "*core platform services*",[3] where each already presents "*apparent and pressing*"[4] concerns about unfair practices by gatekeepers:

- intermediation services (including online marketplaces (e.g., Amazon), app stores (e.g., Google Play, Apple), and vertical search services (e.g., Google Shopping, Google Flights, Hotel Finder));
- search engines (e.g., Google, Bing);
- social networking services (e.g., Facebook, Twitter, Instagram);
- video-sharing platform services (e.g., YouTube, TikTok);
- number-independent interpersonal communications services (e.g., messaging and video-conferencing services such as Skype, WhatsApp, Signal, Slack, Zoom, Teams);
- operating systems (e.g., Windows, iOS, Android, Chrome OS, Smart TVs);
- web browsers (e.g., Chrome, Edge, Firefox);[5]
- virtual assistants (e.g., Siri, Alexa, Cortana);
- cloud computing services (e.g., AWS, Google Cloud, iCloud, Azure); and
- online advertising services, when provided by an undertaking that provides any of the above-mentioned services (e.g., Google AdWords, Google AdSense, Facebook Ads).[6]

Importantly, the Commission can add to or refine this list following a Market Investigation.

3 Gatekeeper Designation: Dominance 2.0

An undertaking is considered to be a gatekeeper when it provides one or more of the above "core platform services" and wields significant and enduring influence over the EU market (or is likely to in the foreseeable future).

Businesses with a market cap (or equivalent) in excess of €75 billion, or an annual EU turnover in excess of €7.5 billion, for the preceding three years will be designated a gatekeeper for each of its core platform services that meet the following qualitative criteria:

(a) the service has "*a **significant impact** on the [EU] market*";

(b) the service has **sufficient reach** to be "*an important gateway for business users to reach end users*"; and

(c) the service "*enjoys an **entrenched and durable position***" (or "*it is foreseeable that it will enjoy such a position in the near future*").

---

[3] See DMA Article 2.2

[4] See DMA Recital 13

[5] Note: the inclusion of web browsers and virtual assistants was relatively last-minute.

[6] In our view, the wording of the online advertising services category leaves some scope for ambiguity. As written, it suggests that an online advertising service is only considered a core platform service when it is provided by an undertaking that also provides one or more of the other core platform services. But this interpretation relies on the comma between "services" and "providers". Without that comma, the DMA could be interpreted as suggesting that all online advertising services are eligible to be core platform services, "including any advertising networks, advertising exchanges and any other advertising intermediation services provided by an undertaking that provides any of the core platform services listed in points (a) to (i)". See also Article 5.2.a for another example of a sub-clause that cannot be removed without substantially changing the meaning of the obligation.

The DMA sets out quantitative thresholds, above which an entity's core platform service shall be presumed to fulfil each of the above criteria:

(a) It is provided in at least three Member States;

(b) It has at least 45 million monthly active EU end users and at least 10,000 yearly active EU business users; and

(c) It has met these minimum user thresholds in each of the last three financial years.

The DMA requires providers of core platform services that meet the thresholds for presumptive gatekeeper designation to notify the Commission of this "*without delay and in any event within 2 months after those thresholds are met*".[7] In practice, of course, many of the core platform services directly impacted by the DMA will have exceeded these thresholds some time ago, and, as a result, the initial deadline will fall 2 months after the DMA becomes active (around June 2023).

Within 45 working days of receiving all of the required information from the prospective gatekeeper, the Commission will issue a *designation decision* formally identifying the gatekeeper's core platform services. Gatekeepers will then be expected to comply with their DMA obligations within six months of this designation decision. Under the current timetable, this could see the first tranche of designated gatekeeper obligations coming into force by January 2024.

Note that the Commission "*shall [also] designate as a gatekeeper*"[8] any core platform service that meets all of the *qualitative* criteria for gatekeeper status, while not (yet) meeting all of the *quantitative* thresholds for presumptive gatekeeper status.[9]

While there will inevitably be disputes around some of the details of the designation process, there is no doubt that the DMA is aimed squarely at the Big Four (Google, Facebook, Apple, and Amazon and, to a lesser extent, the Big Five (which includes Microsoft).

4 Gatekeeper Obligations

The DMA is designed to complement rather than replace existing EU competition rules.[10] Under the current rules, which address anti-competitive practices *after* the event, regulators are required to painstakingly demonstrate that these practices were not objectively justified and had already harmed (or had the potential to harm) competition. In contrast, the DMA aims to deter anti-competitive practices in the first place, by proactively imposing a broad range of obligations on the designated gatekeepers.

But, in addition to shaping the *future* conduct of digital gatekeepers, the DMA will also have a significant impact on their *current* conduct. It prohibits some of the Tech Superpowers' most strategic and lucrative business practices, many of which have been in place for several years. Indeed, "*apparent and pressing concerns*"[11] about these existing practices were often the motivation behind the DMA's obligations.

Neutralising the Tech Superpowers' Most Effective Time-Wasting Strategy

Notably, the DMA also eliminates the efficiency and objective justification defences—excising the notion that the anti-competitive harm caused by these prohibited practices can ever be justified in the hands of a digital gatekeeper. This is likely to be controversial. Indeed, in its comments to the

[7] See Article 3.3
[8] See Article 3.8
[9] See Articles 3.8 and 17
[10] See Recitals 10 and 11
[11] See Recital 13

ACCC, Google has already objected to the DMA's removal of these defences.[12] In our view, this is not because Google believes its practices to be objectively justified. It is because Google recognises that removing its ability to run false efficiency and objective justification arguments will single-handedly neutralise one of its most effective time-wasting strategies.

In a sense, the DMA recognises that, while there might occasionally be minor efficiency gains or user benefits capable of outweighing the anti-competitive effects of these kinds of practices, in the vast majority of cases the complete opposite is true. That is, the DMA prioritises the unquantifiable, but potentially myriad, benefits that will arise from protecting or restoring healthy competition within these fast-moving digital markets, over the quantifiable but often dubious benefits of the gatekeeper practices in question. After all, it is arguments about these supposed benefits and efficiencies that have allowed companies like Google to make a mockery of existing competition law. In the Google Search case, for example, Google has already bought itself years of additional anti-competitive gains by running bogus objective justification arguments through the Commission and the Courts of Appeal. And in the meantime, competition in several vertical search markets has either stagnated or died on the vine.

The DMA's obligations are set out across three Articles. Those in Articles 5 and 6 seem to have been primarily designed to address current practices by digital gatekeepers that already contravene the principles of contestability and fairness. Whereas the obligations set out in Article 7 (which were a late addition that seem to have been largely inspired by lessons learned from the telecoms industry) sets out a number of interoperability obligations for messaging platforms.

As we'll see below, the ability for the Commission to "supplement"[13], update, and "further specify" the DMA's gatekeeper obligations, and to prescribe the specific measures that a gatekeeper must implement in order to "effectively comply"[14] with its obligations are key features of the DMA.

No one could accuse the DMA of a lack of ambition. The obligations it imposes on gatekeepers are far-reaching and complex, and their precise interpretation is likely to be argued and litigated for years. For the purposes of this document, we will focus primarily on the obligations and prohibitions that are most relevant to search engines and/or where we feel that we have particular insights that could contribute to the discussion.

4.1 Article 5 Obligations

4.1.1 Article 5.2 – Closing the GDPR Loopholes

Article 5.2 is designed to protect users' personal data by forbidding digital platforms (such as Facebook and Google) from combining and using data across different services without the users' express and fully informed consent. At a high level, this seems to be aimed at closing some of the GDPR's contract and fair-use loopholes.

4.1.2 Article 5.3 – Prohibiting Most-Favoured-Nation Clauses

Article 5.3 prohibits a digital gatekeeper from imposing most-favoured-nation (MFN) clauses on businesses that participate in its intermediation services. For example, under this obligation, Google's Hotel Finder will no longer be allowed to prevent hotel operators or competing travel search and booking services from offering better prices or conditions through their own websites and apps than they offer through Hotel Finder.

[12] See Google's comments to the Australian ACCC: "The EU's DMA, by contrast, does not expressly allow for such defences…"
[13] See Article 12
[14] See Article 8.2

In some ways, this straightforward and unambiguous obligation goes beyond merely levelling the playing field. It could provide some competing intermediation services (such as Expedia) with an advantage, because they will not be subject to this restriction.

4.1.3 Article 5.4 – Businesses Must be Allowed to Promote Offers and Conclude Contracts

In our view, the wording of Article 5.4 is perilously ambiguous, and the explanatory supporting text set out in recital 38 does little to resolve this ambiguity.

Article 5.4 is comprised of the following single sentence that contains (at least) four subclauses:

> *"The gatekeeper shall allow business users, free of charge, to communicate and promote offers, including under different conditions, to end users acquired via its core platform service or through other channels, and to conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the gatekeeper."*

Unpacking the first half of this sentence, it is clear that gatekeepers must "*allow business users…to communicate and promote offers…to end users*". It is also clear that businesses must be allowed to do this "*free of charge*", and regardless of whether these end users were acquired via the gatekeeper's platform service or through other channels. Moreover, in accordance with the most-favoured-nation obligations set out in Article 5.3, the offers being communicated or promoted to end users can be at prices or conditions that are different from those offered through the gatekeeper's own platform service. All well and good.

But the second half of the sentence, which concerns the conclusion of contracts with end users, is considerably less clear. It *is* clear that the gatekeeper must "*allow business users…to conclude contracts with those end users*" and that it must allow this regardless of whether or not the business uses the gatekeeper's platform for that purpose. But it is *not* necessarily clear whether this conclusion of contracts must also be "*free of charge*"—i.e., without commissions. In our view, a strict grammatical interpretation of the text would suggest that it does mean this. But, if so, this could significantly undermine the business model of App stores and other intermediation services when they are provided by a gatekeeper.

Given the potentially seismic implications of this obligation (and at the risk of beating a dead horse), we suggest that it is worth explicitly setting out the two ways in which the text of Article 5.4 could be interpreted:

Option 1:

The gatekeeper shall allow business users:

a) **free of charge**, to communicate and promote offers, including under different conditions, to end users acquired via its core platform service or through other channels; and
b) to conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the gatekeeper.

Option 2:

The gatekeeper shall allow business users, **free of charge**:

a) to communicate and promote offers, including under different conditions, to end users acquired via its core platform service or through other channels; and
b) to conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the gatekeeper.

If the EU intended the interpretation set out in Option 1, then it could easily have expressed this unambiguously using two separate sentences. For example:

*"The gatekeeper shall allow business users, free of charge, to communicate and promote offers, including under different conditions, to end users acquired via its core platform service or through other channels**. The gatekeeper shall also allow business users** to conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the gatekeeper."*

4.1.4 Article 5.5 – Users Must be Allowed to Access Content & Features Acquired Through 3rd Parties

Gatekeepers must allow users to access and use any content, subscriptions, features or other items acquired through a third-party software application. In a sense, this can be viewed as belt and braces for Article 5.4.

4.1.5 Article 5.6 – Users Must Not Be Prevented from Raising Complaints or Seeking Redress

Gatekeepers must not prevent businesses or users from raising complaints about, or seeking redress for, a gatekeepers' non-compliance with the DMA.

4.1.6 Articles 5.7 and 5.8 – No Bundling, No Tying

Articles 5.7 and 5.8 are the anti-bundling/anti-tying obligations.

Article 5.7 prevents gatekeepers from tying the use of any of its core platform services to its sign-in, browser, or payments services. That is, business and end users of the gatekeeper's core platform service must not be required to also use, offer, or interoperate with the gatekeeper's ancillary services.

Article 5.8 prevents gatekeepers from requiring business or end users of one of its core platform services to subscribe to, or register with, any of its other core platform services.

4.1.7 Articles 5.9 and 5.10 – Transparency of Advertising Fees and Costs

Articles 5.9 and 5.10 require gatekeepers to provide users of its advertising services with detailed information about the costs, fees, and remuneration associated with the advertisements they place or display. The two articles are essentially mirror images of each other—each setting out the data that must be provided (free of charge and on a daily basis) to advertisers and publishers respectively. For every advertisement placed, displayed, or clicked-on, the advertiser and publisher are each entitled to receive a breakdown of:

- what the advertiser paid, including any advertising fees or surcharges;
- what remuneration the publisher received, including any deductions or surcharges; and
- the metrics on which each of these prices, fees and remunerations were calculated.

Where a publisher or advertiser does not consent to the gatekeeper sharing this information for specific advertisements, then the gatekeeper must provide daily averages instead.

This enforced transparency should allow advertisers and publishers to finally see precisely how much of their advertising budgets or revenues are being retained by the gatekeeper, and act accordingly. If gatekeepers, such as Google, fully comply with this obligation it could have a transformative impact on Google's bottom-line and on the online advertising industry as a whole.

4.1.7.1 A Possible Side-Effect of Articles 5.9 and 5.10

The obligations set out in Articles 5.9 and 5.10 mean that advertisers and publishers will both have access to the same data about the particular advertisements they place or publish. But, the particular collections of advertisements for which they have this same or similar data will be very

different. In short, advertisers might be able to spot any systemic inequities in the way that the gatekeeper is treating different publishers, while publishers might be able to spot any systemic inequities in the way that the gatekeeper is treating different advertisers. And this kind of intelligence will be even more actionable if the data is not anonymized (and there is no indication that the DMA expects it to be).

4.2 Article 6 Obligations

The obligations set out in Article 6 are "*susceptible*" to "*being further specified*" by future "*implementing acts*" setting out specific measures that a particular gatekeeper needs to implement in order to "*effectively comply with the obligations*".[15] That is, the DMA anticipates that the obligations in Article 6 might need to be refined and updated[16] in response to changing market conditions or to any attempts by a gatekeeper to disregard or circumvent its obligations.

It should be noted that, while the obligations set out in Article 6 are explicitly flagged as being particularly susceptible to refinement and change, other parts of the act make clear that the obligations set out in Article 7 and, in certain circumstances, those set out in Article 5 (for example, when the Commission "*open[s] proceedings on its own initiative for circumvention*")[17] are also susceptible to refinement and change.

This power to respond rapidly, dynamically and, where necessary, iteratively with prescriptive measures tailored to a gatekeeper's specific activities could prove to be one of the most important features of the DMA (see section 5.3).

4.2.1 Article 6.2 – Gatekeepers Must Not Exploit Data Generated or Provided by its Business Users

Article 6.2 prohibits gatekeepers from using any of the data generated or provided by business users of its core platform (and ancillary) services for the purpose of competing with those business users. This prohibited data includes the aggregated and non-aggregated data that can be inferred from, or collected through, the commercial activities of business users or their customers, including *click*, *search*, *view,* and *voice* data (unless that data is publicly available).

4.2.2 Article 6.3 – Users Must be Free to Choose their Default Search Engine, Virtual Assistant, and Browser

Gatekeepers must allow users to "*easily*" uninstall all software applications from their operating systems (with the exception of applications "*that are essential for the functioning of the operating system*" or the device, and "*which cannot technically be offered on a standalone basis by third parties*").

Gatekeepers must also allow users to "*easily*" change the default settings of their operating systems, virtual assistants, and web browsers whenever those settings "*direct or steer end users to products or services provided by the gatekeeper*". This ability to change defaults must include prompting users to choose "*from a list of the main available service providers*" on their first use of the search engine, virtual assistant, and web browser used by the OS, and of the search engine used by their chosen virtual assistant and web browser.

4.2.2.1 Potential Problems and Unintended Consequences

As far as we can tell, the DMA itself offers no further guidance about what might constitute the "*list of the main available service providers*". And, in our view, the vagueness of this requirement is

[15] See Article 8.2
[16] See Article 12
[17] See Article 8.2(c)

exacerbated by the notable lack of any explicit stipulation that a rival service's appearance in this list must be "*free of charge*".

Without clearly defined rules and procedures for determining, updating, and ordering these lists of *"main available service providers"*, there is a risk that this obligation might in itself become an additional barrier to new entrants and/or a tool by which gatekeepers can cherry-pick their favoured and/or least threatening rivals. We expect these rules and procedures to be clarified in the coming months as part of the Commission's implementation guidelines.[18]

There is also, in our view, a risk that these choice screens could, in some instances, act to further undermine what little competition remains in the search engine and browser markets. This is because some of the leading smaller rivals belong to big players. And, at internet scale, some of these undoubted underdogs may well automatically qualify for gatekeeper status under the DMA's market cap and user thresholds. If so, they would presumably be required to prompt users to switch to an alternative default on first use (including to Google's overwhelmingly dominant search engine and/or Chrome browser). It is easy to imagine that many users that might not ordinarily stray from default settings might switch their default search engine and web browser to Google and Google Chrome if actively offered the choice.

4.2.3 Article 6.4 – Gatekeepers Must Allow and Support 3rd Party App Stores(!)

According to Article 6.4, gatekeepers must "*allow and technically enable the installation and effective use of third-party*" apps and app stores. Gatekeepers must also allow and "*technically enable*" end users to "*easily*" set these third-party apps or app stores as their defaults.

4.2.3.1 Ambiguities and Potential Problems

While Article 6.4 is quite clear that gatekeepers must allow third party apps and app stores to be both installed on their platforms and set as the default, it is not, in our view, as clear about what measures gatekeepers will be allowed to take to protect their ecosystems and users from any harm that might arise from these sometimes highly privileged and potentially malicious applications.

In any event, what is clear is that this obligation is likely to be highly controversial and hotly contested. While opening up previously closed systems, such as Apple's iOS App Store, is likely to lead to increased competition, it is also likely to expose users to the dangers of under-vetted (or even entirely un-vetted) apps from third-party app stores that do not necessarily prioritise user safety or the integrity and privacy of user data.

Moreover, requiring gatekeepers to allow third-party app stores to be installed on their platforms, and even set as the default for all new app downloads and purchases, seems to risk undermining the business model and incentives of these ecosystems. Particularly when these obligations are viewed in conjunction with those set out in Article 5.4 (see section 4.1.3).

4.2.4 Article 6.5 – Search Engines Must Not Favour Their Own Services

Article 6.5 is the much-vaunted search engine non-discrimination obligation. It prohibits search engines (and other gatekeepers, such as app stores and marketplaces) from treating their own services (or products) "*more favourably*" than "*similar*" third party services in their search results. It also requires them to "*apply transparent, fair and non-discriminatory conditions*" to their "*ranking[s]*".

In its June 2017 Google Search (Comparison Shopping) Prohibition Decision, the Commission found that Google gave its own comparison shopping service (CSS) *"more favourable positioning and*

[18] See Recital 95

display" within ***"****its general search results pages"* than rival CSSs. That is, the Decision made clear that *"favouring"* covers both the relative placement of results (positioning), and what these results look like (display). And it also made clear that this applies to the search results page as a whole, irrespective of how these results got there (e.g., whether via the *"rankings"* of Google's generic search algorithms or via the inherent self-dealing of Google's Universal Search mechanism).

The DMA takes a slightly different approach. It prohibits gatekeepers from favouring their products and services "*in ranking and related indexing and crawling*" and leaves the important clarifications about the precise meaning of "*ranking*", "*favouring*", "*search results*", and so on, to the background recitals and the definitions set out in Article 2.

For example, in recital 52 the DMA makes clear that the term ranking "*covers all forms of relative prominence, including display…*". And the definition of the term ranking in Article 2.22 explains that it "*means the relative prominence…or the relevance given to search results by online search engines…irrespective of the technological means used for such presentation [and] organisation…*".

And in Article 2.23, the DMA defines the term "*search results*" as "*mean[ing] any information in any format…returned in response to, and related to, a search query, irrespective of whether the information returned is a paid or an unpaid result, a direct answer or any product, service or information offered in connection with the organic results, or displayed along with or partly or entirely embedded in them*". That is, the DMA broadly mirrors and extends the Search Prohibition Decision—defining search results as the entirety of the search results page (or any other mechanism for delivering search results) generated in response to a query.

In summary, the DMA makes clear that the phrase "*ranking and related indexing and crawling*" covers all of the ways in which search results might be displayed or delivered, as well as any alternatives to generic search ranking algorithms (such as Google's Universal Search mechanism). This last point is further reinforced by supporting recital 52, which states that "*to ensure that this obligation is effective and cannot be circumvented, it should also apply to any measure that has an equivalent effect to the differentiated or preferential treatment in ranking.*"

Moreover, by stipulating that search engine rankings be based on "*transparent, fair and non-discriminatory conditions*", the DMA embraces the concept of Search Neutrality[19] and arguably goes further than the Google Search Decision. And this obligation is further reinforced by Article 6.12, which imposes FRAND conditions of access to search engines by business users (see section 4.2.11).

Finally, because this search engine non-discrimination obligation is contained within Article 6, it is explicitly susceptible to further specification and refinement, which should allow the Commission to respond to any attempts by gatekeepers to move the goalposts or otherwise circumvent this critical obligation.

See also section 4.2.11, where we explain how the combination of this non-discrimination obligation with the FRAND obligation of Article 6.12, should finally put an end to Google's search manipulation practices and the auction-based escalations of these practices that Google has repeatedly offered or implemented in the guise of a "remedy".

4.2.5 Article 6.6 – Users Must Have Unrestricted Access to the Apps and Services of their Choosing

Gatekeepers must not prevent or unduly restrict users from switching to or subscribing to applications and services of their choosing, including as regards their choice of ISP.

[19] See Opinion | Search, but You May Not Find - The New York Times (nytimes.com) or http://www.searchneutrality.org/search-neutrality

4.2.6 Article 6.7 – Interoperability with 3rd Party Devices and Apps

Gatekeepers must allow third-party applications and hardware devices to interoperate with their operating systems and virtual assistants free of charge and in the same way as their own applications and devices. For example, it seems that, under this obligation, Apple must allow third-party applications and devices (such as an Android phone) to pair and interoperate with its Apple Watch in exactly the same way that its iPhones can. It should be noted that, at the time of writing, Apple doesn't even allow this for most of its own hardware devices (such as Apple Macs and iPads).

Furthermore, when a gatekeeper provides services that are ancillary to its core platform service (such as Apps), then it must provide competing providers of such services with the same access to the hardware and software features of its core platform service as are available to the gatekeeper's own services. For example, under this obligation, it seems that Apple must allow third-party providers of Apple Watch apps and watch-face complications to update those complications with the same frequency and level of detail as Apple's own apps can.

Note that gatekeepers are allowed to take any proportionate and duly justified measures that are necessary to ensure that the required interoperability does not compromise the integrity of their hardware, operating system, virtual assistant, or other software.

4.2.7 Article 6.8 – Advertisers & Publishers Must be Provided with the Tools and Data Necessary to Independently Audit the Performance of their Ad Campaigns and Inventory

In essence, Article 6.8 requires gatekeepers to provide advertisers and publishers with access to the tools and data necessary to conduct their own independent assessment of the performance of the advertisements they place and/or publish. Moreover, access to these tools and data must be provided free of charge.

In other words, gatekeepers must provide advertisers and publishers with the information needed to verify (and, when necessary, dispute) any assessments or performance summaries provided to them by the gatekeeper. For example, we would expect this data to include how often ads were shown, where they were shown and under what circumstances, how often they were clicked on, where the clicks came from (i.e., to help identify click fraud), the extent to which the cost of the ads deviated from their bids, and so on.

4.2.8 Article 6.9 – Data Portability and Multi-Homing for Users

Gatekeepers must provide users (and their authorised agents) with continuous and real-time access to any data provided or generated by the user's activities on the relevant core platform service. Gatekeepers must provide this data, along with the tools required to facilitate its portability, free of charge.

4.2.9 Article 6.10 – Data Portability and Multi-Homing for Businesses

The wording of Article 6.10 is a good example of the hazards of designing, not just by committee, but by a committee of committees (in this case, the European Commission, Parliament, and Council). But, in essence, where Article 6.9 provides for data portability and multi-homing for end users, Article 6.10 provides the same for businesses.

For example, this obligation should ensure that advertisers can easily move their advertising campaigns from one platform to another (portability) or manage their campaigns on multiple platforms at once via a single interface or ad agency (multi-homing).

4.2.10 Article 6.11 – Search Data Must be Shared with 3rd Party Search Engines

A search engine gatekeeper must provide third-party search engines with access to its "*ranking, query, click and view data*" on fair, reasonable and non-discriminatory terms (FRAND). This data must be provided on request and must cover all such data "*generated by end users on [the gatekeeper's] online search engines*" in relation to both "*free and paid search*".

We note that this obligation for Google to provide rival search engines with access to this vast treasure trove of search-related data carries no stipulation that it be provided "*free of charge*" or within certain timescales. Ultimately, the effectiveness of this obligation will therefore depend on how Google and/or the Commission determine what constitutes a "*fair and reasonable*" basis for third parties to obtain (and possibly pay for) this kind of data.

4.2.11 Article 6.12 – FRAND Access to App Stores, Search Engines, and Social Networks

Article 6.12 requires gatekeepers to provide businesses with fair, reasonable, and non-discriminatory access to their app stores, search engines, and social networking services. It also requires gatekeepers to "*publish*" these "*general conditions of access*" (which must include "*an alternative dispute settlement mechanism*"), so that the Commission can assess whether these conditions comply with the obligation.

This obligation was originally conceived and developed with app stores in mind, and clear signs of its app-store-centric origins remain in background recital 62. But at the March 2022 trialogue (where the European Commission, Parliament, and Council met to thrash out the details of the act), the scope of the obligation was expanded to (explicitly) include search engines and social networks.

4.2.11.1 The Implications for Search Engines

The implications of this FRAND obligation for app stores are relatively straightforward. For example, app store gatekeepers cannot impose unfair or unreasonable conditions, charge unreasonable or "*disproportionate*" commissions, or unfairly favour their own apps over rival apps.

The implications for search engine gatekeepers (i.e., Google), while not quite so straightforward, could prove to be significantly more consequential. For example, if properly applied, this FRAND obligation becomes yet another way in which Google's consumer-hostile and brazenly anti-competitive CSS Auction is unlawful.

So, what does "*fair, reasonable, and non-discriminatory general conditions of access for business users*" mean within the context of a search engine?

First, clearly, "*access*" to a search engine in this context does not mean being able to perform searches; it means being listed within the search engine's search results. And the DMA's definition of "*search results*" (in Article 2.23) makes clear that these include both free and paid listings.

Second, because the non-discriminatory aspects of these FRAND conditions are already covered by Article 6.5, we only need to consider what the additional constraints of "*fair*" and "*reasonable*" means in the context of both free and paid listings.

4.2.11.2 "Fair and Reasonable" Access to a Search Engine's Free/Organic Search Results

In the context of free, relevance-based, organic search results, "*fair and reasonable*" access can only mean non-discriminatory inclusion and placement, free of charge, and based solely on relevance. Apart from anything else, charging businesses to appear within a search engine's free listings would be a contradiction in terms.

But it also means not making a business's inclusion within search results contingent on any unfair or unreasonable conditions. For example, it would not be fair or reasonable to make news publishers'

eligibility to appear within Google's natural search results contingent on their allowing their content to also appear within Google News.

Moreover, we suggest that this obligation also prohibits search engines from applying anti-competitive and/or objectively unfair algorithmic search penalties, such as those that Google uses to systematically demote rival CSSs. Clearly, penalising a business (let alone one that is a direct competitor to one of Google's own services) on the basis of characteristics (such as a lack of original content, and a primary purpose to direct users to other websites) that are inherent to these kinds of services (including Google's own) is both objectively unfair and unreasonable. And, of course, it also falls foul of the non-discrimination stipulations, both in this Article and in Article 6.5.

4.2.11.3 "Fair and Reasonable" Access to a Search Engine's Pay-for-Placement Advertisements

The second paragraph of recital 62 states that:

> *"Pricing or other general access conditions should be considered unfair if they lead to an imbalance of rights and obligations imposed on business users or confer an advantage on the gatekeeper which is disproportionate to the service provided by the gatekeeper to business users or lead to a disadvantage for business users in providing the same or similar services as the gatekeeper."*

In the context of a search engine's paid listings, this means that search engines cannot charge a business a proportion of their profits that is "*disproportionate to the service [being] provided [to the business] by the gatekeeper*". This could prove highly problematic for Google, because the economics of its pay-for-placement auctions inevitably drives prices up to the maximum that advertisers can afford to pay whenever there are more bidders than available slots (i.e., whenever the auction is over-subscribed).[20] And, because most high-value search terms *are* over-subscribed (often substantially so), advertisers typically end up paying Google 80-95% of their anticipated profit.

Moreover, the stipulation that search engines cannot use "*pricing or other general access conditions*" that "*lead to a disadvantage*" for business users "*providing the same or similar services*" as the gatekeeper is also highly problematic for Google. Google's woefully non-compliant CSS Auction, which already falls far short of the equal-treatment remedy mandated by the EC's June 2017 Prohibition Decision, clearly falls foul of this (and the previous) stipulation. That is, Google's CSS Auction compels participants to bid away a disproportionate 80-95% of their anticipated profit (and hand it to Google). And, because the bids of Google's own CSS are merely internal accounting (where every "*cost*" has a corresponding and equal "*credit*"), this clearly leads to a substantial disadvantage for rival CSSs compared to Google's own CSS. [21]

And, given that Article 8.8 specifically obligates the Commission to confirm that the measures taken to comply with Article 6.12 have removed any "*imbalance*", restored a level playing field, and "*do not [in] themselves confer an advantage on the gatekeeper*", we should all expect Google's CSS Auction to be summarily rejected in due course for failing to comply with Article 6.12.

Finally, it is important to note that Google has not yet taken any steps to deactivate its anti-competitively applied, CSS-demoting penalty algorithms. As a result, for the five years since the EC's June 2017 Prohibition Decision, rival CSSs have continued to be denied meaningful access to

[20] See Section 2.3 of our Response to the EC's Pre-Rejection Letter and https://pubs.aeaweb.org/doi/pdfplus/10.1257/aer.99.2.430

[21] For more details, please see: http://www.foundem.co.uk/fmedia/Foundem_Apr_2018_Final_Debunking_of_Google_Auction_Remedy/ and http://www.foundem.co.uk/fmedia/Foundem_Google_CSS_Auction_Revenue_Counts_As_Traffic_Nov_2019/

Google's free, relevance-based, search results, and their access to Google's paid listings (via Google's CSS Auction) has clearly been both disproportionately expensive and conferring of an unfair advantage on Google's CSS. After all, as a direct result of Google's CSS Auction, Google's CSS is now the only CSS in Europe that does not have to pay at all, let alone "*disproportionately*", for access to Google's search engine.

4.2.11.4 Pre-Empting Any Arguments About the Term "In particular"

We anticipate that some gatekeepers, such as Google, might seize on the use of the term "*in particular*" in the middle of the first paragraph of recital 62 to try to argue that the onerous "*fair and reasonable*" pricing requirements discussed above are only supposed to apply to app stores.

However, the first thing to note is that the DMA often uses the term "*in particular*" to mean "*including*", "*especially*", or "*for example*".[22]

Moreover, in this case, the DMA's use of the term "*in particular*" is clearly merely a relic of the way in which this obligation evolved over time—i.e., before its scope was explicitly extended beyond app stores to include search engines and social networks.

Finally, all of the qualities cited by recital 62 following the "*in particular*"—namely that app stores are an important gateway for business users that seek to reach end users and that there is an "*imbalance in bargaining power*" between the gatekeeper and business users—apply equally (if not more so) to search engines.

4.2.12 Article 6.13 – Unsubscribing Must Not Be Unnecessarily Difficult or Complicated

A gatekeeper must not make it unnecessarily difficult or complicated for its business or end users to unsubscribe from its core platform service. For example, closing an account or unsubscribing from a service should not be more complicated or onerous than opening an account or subscribing to the same service.

4.3 Article 7 Obligations

The nine obligations set out in Article 7 oblige providers of number-independent interpersonal communications services (i.e., messaging and video-conferencing services such as WhatsApp, Signal, Teams, and Zoom) to ensure that they are interoperable with each other and new entrants, "upon request, and free of charge."

These interoperability obligations phase in over a period of four years from gatekeeper designation, starting with the necessary technical interfaces to allow end-to-end text messaging and file sharing between two individual end users. This obligation then extends to groups of users within two years of designation, and culminates in support for full voice and video calls between individuals and groups of users within four years of designation.

5 Enforcement

Of course, the DMA will only be effective if gatekeepers comply with their obligations, which history shows they are often reluctant to do. Particularly when one considers just how lucrative many of these practices are and how fundamental to the gatekeepers' business models and/or growth strategies. Put simply, some of the tech superpowers are now "too big to care"; they are only likely to comply if they believe that the consequences of non-compliance will outweigh the benefits.

[22] For example, see: https://www .adamsdrafting.com/in-particular/

Fortunately, the DMA provides substantial enforcement powers and sanctions that, if utilised, should tip the scales in favour of compliance.

As discussed in the Introduction, in a sense the DMA can be viewed as a collection of pre-packaged, but at this point fine-less, Prohibition Decisions that put designated gatekeepers on notice that certain of their business practices (many of which have been in place for several years) have now been deemed unlawful. As with Prohibition Decisions, gatekeepers are required to end (or refrain from) these prohibited practices or face non-compliance proceedings.

By deeming many of the most harmful business practices of the digital age unlawful on their face, and by abrogating the need to either define markets or establish dominance within those markets, the DMA provides a fast-track for bringing these practices to an end. This is in stark contrast to the tools available under Article 102, where achieving anything comparable would take decades. Moreover, by neutering the ability for gatekeepers to run down the clock making vacuous objective justification and efficiency defences (as has happened repeatedly, for example, in the Google Search case), the DMA should further accelerate the path to compliance.

A full analysis of the DMA's sanctions and enforcement powers is beyond the scope of this document, so we focus below on those aspects where we have particular insights that we feel could contribute to the discussion.

5.1 Escalating Sanctions for Repeat Offenders

As with the adoption of a Prohibition Decision, once a gatekeeper has been formally designated the clock starts ticking for compliance. In the case of the DMA, the gatekeeper has **six months** to bring its core platform service or services into line with all applicable obligations.[23]

Under the DMA, the sanctions for non-compliance are considerable and allow for rapid escalation for repeat offenders. For example, the Commission can impose fines of up to 10% of the gatekeeper's worldwide annual turnover in the case of non-compliance with one of the obligations, and up to 20% in the case of repeated infringements (i.e., a repeat of the same or similar non-compliance within eight years).[24] In addition, the Commission can impose periodic penalty payments of up to 5% of annual turnover in cases where the gatekeeper continues to fail to comply following a non-compliance decision.[25]

Moreover, for cases of "*systematic non-compliance*"—where a gatekeeper has failed to comply with its obligations across one or more of its core platform services three times within an eight-year period—the gatekeeper could then face the "*the ultimate remedy of divestitures and structural separation*".[26]

5.2 Interim Measures 2.0 (Article 24)

The Commission's ability to bring a swift end to a gatekeeper's unlawful practices should be further enhanced by the DMA's simpler and (from the Commission's point of view) considerably less hazardous path to injunctive relief through the imposition of interim measures.

Historically, interim measures have rarely been used, and there is a consensus among commentators that this is likely to remain the case under the DMA. This is primarily because the bar to deploying interim measures remains superficially the same: a prima facie finding of infringement and a risk of "*serious and irreparable*" harm if the gatekeeper's practices are left unchecked. But there is an

[23] See Article 3.10
[24] See Article 30
[25] See Article 31
[26] See Article 18 and https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_4327

important difference between the provisions for interim measures under Article 102 and their counterparts under the DMA. And this difference could (and, in our view, should) resuscitate this under-utilised and potentially game-changing enforcement tool.

The critical difference arises from where in the process these interim measures will be deployed.

Under Article 102, the imposition of interim measures would typically occur in the early stages of a multi-year investigation that may or may not ultimately culminate in a Prohibition (or Commitments) Decision. In effect, the Commission is required to gamble that its investigation will eventually establish that the undertaking is dominant in the relevant market; that the practices under investigation really have harmed (or have the potential to harm) competition; and that these findings will withstand the undertaking's extensive rights of defence, including any objective justification or efficiency arguments.

By contrast, as discussed above, when the Commission designates an undertaking as a gatekeeper, it is effectively serving it with the broad equivalent of a Prohibition Decision. As a result, under the DMA the imposition of interim measures occurs when the Commission is effectively at the *end* of the equivalent of an Article 102 investigation and is now *only* concerned with compliance.

Moreover, because the Commission will only be considering interim measures at the point where it has already decided that there is a prima facie case that the gatekeeper is not complying with one or more of its obligations, the only remaining hurdle to fulfilling the requirements for interim measures is the risk of "serious and irreparable" harm that would be posed by inaction. And, crucially, in many cases this too will already have been predetermined by the DMA. That is, there will often be an implicit assumption that failing to comply with one of the DMA's obligations is likely to cause serious and irreparable harm, because otherwise it would not have been included as an obligation.

If nothing else, this low-risk, low-barrier path to interim measures should serve as an effective stick with which to beat recalcitrant gatekeepers into abiding by their obligations. Whereas, under Article 102, the Commission's palpable fear of pursuing interim measures—even in circumstances such as the Google Search case, where the irreparable and ongoing cost of inaction to businesses and consumers was painfully clear throughout—only serves to embolden the undertaking under investigation.

5.3 Ensuring the Effectiveness of the DMA

Many of the DMA's provisions are aimed at ensuring that the measures taken by gatekeepers to comply with their obligations are effective[27], including, where necessary, by being highly prescriptive about precisely what those measures should be.[28] Other DMA provisions are aimed at allowing it to stay abreast of developments[29] and respond to any attempts to circumvent it.[30]

In essence, the DMA is structured so that: if the specified list of core platform services prove insufficient or ineffective, then the Commission can add additional platform services; and if the specified obligations prove insufficient or ineffective, then the Commission can refine or amend those obligations; and if what the Commission has instructed a gatekeeper to do proves insufficient or ineffective, then it can even change its mind and tell the gatekeeper to do something else as well or instead.

This ability to refine and update the operative elements of the DMA, and to respond to any attempts by gatekeepers to circumvent their obligations or move the goalposts, could prove to be one of its

[27] For example, see Article 8.1
[28] For example, see Articles 12.2(c) and 13.7
[29] See Articles 12 and 19
[30] See Article 13

most significant features. As could the explicit ability for the Commission to ensure and, where necessary iterate towards, truly effective remedies.

Moreover, in stark contrast to Article 102, the DMA imposes strict time limits on the various stages of the enforcement process. For example, when the Commission opens proceedings with a view to the possible adoption of a non-compliance decision, it is required to conclude those proceedings within 6 months and to publish a Report explaining the measures that it considers the gatekeeper should take within 3 months.

5.4 Enforcement Through Transparency

The DMA includes several explicit transparency obligations. For example, Article 6.5 requires gatekeepers to "*apply transparent, fair and non-discriminatory conditions*" to its search results. And Article 6.12 requires gatekeepers to publish their general conditions of access, so that the Commission (and others) can assess whether they meet their obligation to be fair, reasonable, and non-discriminatory. And Articles 11.1 and 11.2 require gatekeepers to provide the Commission with a detailed and *transparent* report describing the measures it has implemented to ensure compliance, as well as to *publish* a non-confidential summary of this report.

In our view, transparency is a particularly important element of enforcement in digital markets. Because with transparency comes expert scrutiny. And in these often-complex technology markets, that expert scrutiny can prove decisive—a point that was repeatedly demonstrated throughout the Google Search case.[31]

And, as we wrote in a January 2013 White Paper, transparency does not necessarily mean access to the details of a gatekeeper's business practices or algorithms. In most cases, simply scrutinising the rationale behind these practices and algorithms will be sufficient to assess their objectives, legitimacy, fairness and likely impact. For example, our January 2013 paper set out a robust and reliable mechanism for assessing the legitimacy and fairness of any particular algorithmic search penalty, based solely on the answers to four readily answerable questions.[32]

It is difficult to overstate just how important this greater transparency might prove to be in determining the efficacy of the DMA. For example, in our view (and experience), a sizeable proportion of the Commission's seven-year Google Search investigation could have been saved if Google's fundamental misrepresentations of many of the most basic facts of the case had been subjected to expert scrutiny far earlier in the process.

[31] For some publicly available examples, please see: our June 2014 Reply to the EC's Pre-Rejection letter, our March 2014 Open Letter to Commissioner Almunia, our June 2015 Rebuttal of Google's public response to the EC's Statement of Objections, our December 2016 Rebuttal of Google's public response to the EC's Supplementary Statement of Objections, and our April 2016 Analysis of the pivotal evidence in the Streetmap trial.

[32] See "The Test of a Legitimate Penalty" on page 5 of http://www.foundem.co.uk/Enabling_an_Anti-Demotion_Remedy.pdf