Kluwer Competition Law Blog

Amazon's DMA Compliance Workshop – The Power of No: Customer-Obsessed Pathos

Alba Ribera Martínez (Deputy Editor) (University Carlos III of Madrid, Spain) · Thursday, March 21st, 2024

The Digital Markets Act (DMA) became entirely applicable on 7 March 2024. By then, the gatekeepers issued their compliance reports documenting their technical solutions and implementation of the DMA's provisions under Article 11 DMA as well as their reports on consumer profiling techniques as required under Article 15 DMA (see here).

I will be covering the workshops organised by the European Commission per each of the gatekeepers under The Power of No series, where the representatives of the undertakings meet with stakeholders to grind their compliance strategies and solutions. This blog post covers the third workshop organised by the EC for assessing Amazon's compliance solutions. Find here the review of the first workshop relating to Apple's technical implementation and here my comment on Meta's presentation of its compliance plans for complying with the rules in the DMA.

A short summary of the compliance report, a detailed presentation of its compliance plan

On the 7th of March, Amazon delivered quite a summarised version of the solutions that it was planning to roll out as a consequence of DMA implementation. As opposed to 400-page-long censured compliance reports belonging to other gatekeepers, Amazon's own compliance plan was quite brief in terms of the particular details that it sought to put forward for each one of the regulation's provisions.

However, the gatekeeper's approach towards its compliance workshop has been completely different, in terms of form and substance. Amazon's representatives were keen throughout in detailing each of the legal and technical requirements that it would apply to descend each one of the DMA's mandates into reality, especially in the key areas of the use (and the prohibition of its use) of personal and non-personal end user and business users' data across its core platform services (CPSs).

The piece covers Amazon's detailed approach towards i) its technical implementation of Article 5(2); ii) its data portability and access obligations under Articles 6(9) and 6(10) DMA; iii) its advertising transparency obligations enshrined in Articles 5(9), 5(10) and 6(8) DMA and, finally iv) Amazon's use of seller data and its capacity to self-preference across its CPSs abiding by

Articles 6(2) and 6(5) DMA.

The Store and the Ads prompt: cookie-banner-like prompts for a comprehensive choice

As many other gatekeepers have presented in the European Commission's workshops, Amazon thinks around the prohibition under Article 5(2) DMA as a manner to authorise its data combination and cross-use activities via consent screens. This is the same approach, for instance, to Meta's perspective on providing that choice, albeit with huge differences between both models. Amazon first stressed that it does not track customers' browsing activities, nor does it sell its customer's personal data to third parties (as other gatekeepers do, the underlying tone went) since it does not cross-subsidise for catering to its services in this way. This first idea was salient throughout the workshop insofar as Amazon presented itself as a not-purely-digital gatekeeper, given that it intermediates sales for third-party sellers on its marketplace besides its own products via Amazon Retail. In that sense, it merges the best of both worlds in the mix of offline retail and online intermediation of services.

For the particular case of compliance with Article 5(2) DMA, Amazon expanded on the double set of prompts that it designed to provide for a consent moment for users to agree or reject data combinations across its services. Each one of the prompts corresponds with each one of Amazon's CPSs: Amazon marketplace and Amazon Advertising.

The Store prompt asks the consumer whether she wishes that her personal data remain combined and cross-used with other services that are completely unrelated to Amazon's marketplace. For instance, whether the personal data stored as a consequence of the consumer's use of virtual assistant Alexa may, in turn, impact Amazon's experience on the listings of different products across the Marketplace.

As opposed to the rest of the gatekeepers, Amazon has not framed the consent screens as a binary choice but as a third-way selection that the end user may perform in the form of pressing the yellow button 'accept', the plain 'decline' button or the 'customise and learn more' functionality that leads the consumer to perform a more granular choice on what types of data can be linked or not with Amazon's marketplace. According to user flows shown by Amazon in the workshop, the granular choice will mean that the end user must affirmatively choose whether to link Amazon's marketplace data with Alexa, Amazon device services (and the end user may learn more about what products are comprised under the definition through an additional link), its entertainment services (one would say, Amazon Prime Video would fall within scope) and with 'other' Amazon services. In this same vein, the Ads prompt also offers the same choice to the end user but its impact relates to the interaction between Amazon's data (outside of the scope of the DMA) and the gatekeeper's to perform personalised advertising or content through its services.

Asked by BEUC's representative attending the workshop, Amazon recognised that it had venality relied on the format of cookie banners to design its prompts given its positive experience in displaying. One would say, however, that the same positivity may not be so evident if data protection authorities are asked.

From the technical perspective, Amazon also went to great lengths to establish the safeguards that it has implemented to honour the customer's preferences across its technical systems, stemming from the backend of its infrastructure. As soon as the end user makes a choice on the consent

screen, all of the data generated by the end user in the context of Amazon's services are classified and labelled according to the services in which they belong into a central data store. Those credentials are, thus, associated with the customer's ID if the end user is logged in to an Amazon account or to a session ID if the user is not logged into a particular account.

Building upon the labelling of the data, then data access layers apply across Amazon's services so that the end user's preferences are respected. For instance, if an end user has rejected to link its personal data from Amazon's marketplace to the rest of its services, and that same end user accesses Amazon Prime Video, the data access layer will check the consumer's consent selection by retrieving it from the central data store. After that, the data access layer will deliver a response on which services the end user consented for personal data combination in relation to the service that Amazon wants to use to present a personalised experience. In such a case, Amazon will deny the decision based on those checks, so that the content displayed on Prime Video will not be based on the end user's personal data generated across its use of the Amazon marketplace.

Data portability and access obligations: (maybe) not the whole picture

Amazon's presentation on its compliance plan on Articles 6(9) and 6(10) expanded on the brief descriptions that it had formerly established within its summarised version of the compliance report it delivered to the European Commission on the 5th of March 2024.

Similarly to other gatekeepers such as Apple who took the same stance with reference to data portability, Amazon has developed two distinct tools from scratch to comply with the DMA's provisions: the Portability API and the Transfer Your Data Portal. The latter is a self-service webpage where end users can download a copy of their data by accessing the service via their account page. They can then choose the degree of granularity that the download will perform.

The Portability API solution, however, faced more backlash coming from participants of the workshop than it provided certainty. As opposed to the Transfer Your Data Portal's scope in catering portability directly to end users, the Portability API is the dedicated solution that Amazon has worked out to provide third parties with the possibility to port data from the end users upon their authorisation. The right to data portability is not given for granted, as per Amazon's compliance solution. Instead, even if they have received direct authorisation from the end user side, they must request access to call that API to Amazon through a designated workspace.

During that request process, Amazon has vested upon itself the capacity to perform distinct types of internal verification, depending on the types of data that the third party wants to call via the API. In case the third party wishes to access Category 1 data, including public customer data such as product reviews, the request process and verification are somewhat more alleviated. Amazon recognised that this process may take a few weeks to complete. Notwithstanding, if the third party is authorised to access Category 2 data including, for example, the end user's shopping preferences, then a complete privacy and security verification will be run by Amazon upon the third party to understand the third party's privacy and security practices concerning their capacity to assess and protect those values in the event of a data breach. If the request for access is granted, then the third party can call the API on a regular basis.

To several questions asked by stakeholders, Amazon confirmed that it does not intend to impose

additional restrictions on third parties to gain verification under the Portability API solution. Additionally, Amazon pointed out that even if it rejected a third party's request beforehand, it would not automatically hinder subsequent requests for access, which would be examined on their own merits afresh. In turn, it has not introduced a formal dispute resolution mechanism to apply to third parties when such data access is denied.

Under the Portability API solution, Amazon does not lose its grip on end users. In fact, Amazon will present end users with dedicated warnings to alert end users of their choice in authorising third parties.

As of the compliance date (and even, as of the compliance workshop's date), the Portability API solution has not yet been fully rolled out by Amazon, given that most data types are missing within the webpage. On this same point, however, one must remark that Amazon incurred in contradiction with respect to the information that it has made available to its business and end users. According to Amazon on its website, "*Amazon Data Portability enables customers to programmatically port to authorized third party apps or websites portions of their Amazon data from the following marketplaces: Belgium, France, Germany, Italy, Netherlands, Poland, Spain, and Sweden*". Even if one is not too good in maths, those marketplaces do not add up to the 27 Member States that the DMA intends to cover. When directly enquired on whether the Portability API currently covers all EU storefronts, Amazon confirmed that it would. One could add: maybe not yet.

Amazon's compliance solution under Article 6(10) DMA, however, went mostly under the radar, although it seeks to substantially improve existing data access via a new report documenting end user data access authorised via consent (not consent in the sense of Article 5(2) DMA), with continuous access and request through Seller API at any time. The only caveat of Amazon's compliance solution around the provision is that the customer shall independently verify the seller's privacy policy to consent to the documentation being displayed to the business user.

Transparency reports for advertisers and publishers, albeit overriding rejection of consent

In a blog post published in January 2024, Amazon already remarked on the changes that it would introduce as a response to the DMA within its Amazon Ads CPS. During the workshop, it briefly reviewed the reports that it already provides to both advertisers and publishers free of charge, such as the information it already shares with advertisers and publishers on third-party fees or on the total number of times an ad was seen or clicked on.

Regarding pricing transparency, Amazon has extended the granularity of its existing reports on those campaigns aimed at EU users paid by advertisers and publishers using Amazon Ads. The main point of contention around the force of the remedy proposed by Amazon is that of the crossed consents that advertisers and publishers must grant so that all information is available to them. For instance, it may well be the case that, even with the enhanced granularity presented by Amazon, if the advertisers do not consent for its advertiser name and pricing information to be passed on to any publisher, then that same pricing information may only be able for publishers in the form of default aggregated metrics. Amazon responded affirmatively that consents for authorising publishers and/or advertisers are not displayed or granted per advertiser/publisher but in the abstract. Circling back to the example, if the advertiser does not grant consent for the passing on of any information, then not one of the publishers interacting with that same advertiser will be

provided with complete information regarding the pricing information of the ad transactions performed via Amazon Ads with that same advertiser.

On the side of the metrics relating to performance that Amazon Ads must make available by applying Article 6(8) DMA, Amazon introduced in March a new dedicated secure data environment (i.e., a clean room) so that advertisers can verify the measurement of campaigns with granular data on EU-based campaigns. Stemming from that exchange, publishers and advertisers may pass on that same information to third parties without any other limitation.

(Mis)placed trust: use of non-public seller data and self-preferencing

Amazon quickly reviewed via a narrow interpretation of Articles 6(2) and 6(5) DMA that it did not violate any of those provisions. The presentation, however, seemed somewhat surprising against the background of past cases triggered by the European Commission on both these counts, especially regarding Amazon's Buy Box and Prime programme cases that were resolved via commitments offered by the gatekeeper.

The undertaking recalled that those commitments submitted in December 2022 already had in mind the DMA's application. Therefore, no major developments could be expected from it to deliver on the yardstick of refraining from using non-public seller data and self-preferencing its products vis-à-vis those of its competitors.

In general, Amazon only identified three potential areas of conflict where it directly competed with business users relating to the provision of its Amazon marketplace: i) selection decisions (that is, identifying Retail business opportunities and missing gaps, the negotiation with suppliers to satisfy demand and buying decisions); ii) inventory decisions (decisions relating to the quantities to purchase and the management of stock levels); and iii) pricing decisions. Amazon thoroughly reviewed its decision-making process (as well as the functioning of its algorithms) in the use of non-public seller data in competition with third-party sellers and determined, as a result, that it did not use any of that data for them. The outcomes of those decisions were merely based on publicly available data. Thus, any other potential competitor could reach the same conclusions in making those decisions, even if it was not the holder of the whole marketplace. On the side of Amazon Ads, the gatekeeper did not even identify any potential areas of conflict where it competes with business users, insofar as it does not participate in the real-time auctions that business users engage in so as to display their products on Amazon's sponsored and prominent placement within the product's listing.

In a similar vein, the considerations around the application of the prohibition of self-preferencing under Article 6(5) followed the same path. In all of those instances where Amazon could be said to compete with third-party sellers for a product, it confirmed that it only applied objective and relevant criteria on its algorithms to perform its ranking and listing of products. Building upon the rationale of the Buy Box case, Amazon reinstated that none of those decisions were based on the logistics, brand or delivery of the seller that catered to that particular product, but on the merits of each one of the offers displayed directly to the user.

Key takeaways

For some quick moments, one could presume that Amazon's compliance workshop was nothing but straightforward. Nothing further from reality. Amazon's legal and engineering teams prepared well in advance of the workshop and acted as a common front towards participants in the workshop.

However, the gatekeeper's caveated approach in presenting its compliance solutions must still undergo the European Commission's review, so that all of the legal work that the gatekeeper has dedicated to interpreting the DMA is not only legally accurate but factually credible and workable. In some instances, this did not seem to be the case, notably for Amazon's solution surrounding its Portability API to authorise third parties to port data across to their services upon the authorisation of end users. At least, one would expect that the short(-ened) version of Amazon's compliance report would profit from further clarification on some points and further updating as soon as the functionality is effectively rolled out for the benefit of both business and end users.

To make sure you do not miss out on regular updates from the Kluwer Competition Law Blog, please subscribe here.

This entry was posted on Thursday, March 21st, 2024 at 8:30 am and is filed under Algorithms, Amazon, Designation Decision, Digital, Digital competition, Digital economy, Digital markets, Digital Markets Act
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.