

INTERNAL MARKET AND CONSUMER PROTECTION (IMCO)

BACKGROUND PAPER

Workshop

The Digital Services Act and the Digital Markets Act: A forward-looking and consumer-centred perspective

Chair: Anna Cavazzini (MEP)

26 May 2021, 16.45 – 18.45

Introduction

The workshop aims to explore possible conclusions and recommendations on the Digital Services Act (DSA) and Digital Markets Act (DMA) proposals and gather evidence on the expected effects of the regulation of online intermediaries. The discussions of the workshop aim to feed into the DSA and the DMA reports of the IMCO committee, setting out the Parliament's political response. The aim of the first panel is to explore more in-depth some of the issues covered by the DSA proposal, namely the fragmentation of the single market for services, the responsibilities of intermediaries and problems faced by consumers when using online platforms and digital services or accessing illegal services or products, as well as issues related to supervision and enforcement. The aim of the second panel is to explore more in-depth some of the issues covered by the DMA proposal, namely the role that a few online platforms play in the digital economy and the need to ensure a fair and contestable online platform environment to the benefit of consumers. The purpose of the present background paper is to outline the main points that will be discussed by the speakers during the workshop.

Topic 1 of the DSA: Responsibilities of online intermediaries and new due diligence obligations

(Prof. Joris van Hoboken, Vrije Universiteit Brussel and University of Amsterdam)¹

In this short note, I will provide comments on a select number of issues in the proposal of the DSA. After a short discussion of the known legal and policy issues with regard to the current framework for intermediary liability, content moderation and the tackling of illegal content online, I will provide specific comments on the proposed safe harbour provisions for intermediary services, the approach for additional due diligence obligations for intermediary services and online platforms, and the new provisions with regard to online advertising.

1. Known legal and policy issues

There are a variety of known **issues with regard to the existing EU intermediary liability framework** and the responsibility and proper procedures for addressing illegal content in the internal market and the Member States. These issues include the following:

- Significant legal fragmentation with regard to the safe harbours and associated standards;
- Lack of clarity about the scope of EU level statutory safe harbours, in particular for hosting service activity, and the status of key services in the internet service ecosystem;
- Legal uncertainty about the legal consequences of voluntary activity by intermediary services to address illegal content, or content violating Terms of Service;
- Significant questions about the protection of people when using online services, including the way in which current platform policies and notice and action procedures lack adequate safeguards in case of removals or other account-related measures (transparency, due process, fairness, non-discrimination, freedom of expression);
- A lack of accountability, transparency and regulatory oversight and significant information asymmetries between dominant service providers on the one hand, and regulators, civil society, researchers and the general public on the other hand.

In my assessment, the **DSA proposal comes a long way in making significant progress on these issues**. The proposal builds on years of experience with the current legal framework, the functioning of self-regulatory frameworks and legal dynamics in the Member States. At the same time, the subject matter is complex and the challenges of introducing more robust public interest driven regulation and oversight for content moderation in the EU are significant. While the EU has the potential to set a meaningful standard for intermediary liability and content moderation standards with this new legislation, it is paramount that the legislator considers the way in which EU standards are likely to interact with intermediary service operations, legal frameworks elsewhere, and existing law and regulation at EU and Member States level.

2. Safe harbours for intermediary services, definitions and due diligence obligations

By and large the existing EU level framework of safe harbours is copied directly into the DSA proposal, without too many significant changes. This reflects that the need for a harmonized EU level safe harbour for essential intermediary service activities remains essential for the European internal market. The prohibition

¹ For this background note, I have drawn on the work carried out in the context of the [DSA Observatory project](#) at the Institute for Information Law, including by Ilaria Buri, Paddy Leerksen, Ronan Fahy, Natali Helberger, Martin Senftleben, João Pedro Quintais, and Tom Dobber. Specific analysis of DSA related issues will be posted on the website of the project in the coming weeks and months.

of general monitoring obligations is included without amendment. One specific new carve out for e-commerce activity and consumer law is inserted in Article 5's safe harbour for hosting activities, excluding activity that reasonable consumers would believe to be carried out under the authority or control of the respective service provider.

This basic design in the proposed safe harbour set up has the benefit of **continuity and simplicity**. As it provides the foundation for the complementary framework of due diligence obligations (intermediary services, hosting services, and online platforms), it's important to carefully consider any potential lack of clarity about the scope of the definitions.

Some of the known issues with regard to the scope of the safe harbours are addressed by the proposal. In particular, some key issues with regard to the requirement for hosting providers not to play an 'active role' are addressed. The proposal codifies the case law of the Court of Justice of the European Union (CJEU) on the requirement that hosting providers do not play an active role, into the recitals of the proposal (in particular Recital 18) in a way that resolves existing problems. The legal situation that a particular hosting intermediary is too active to be able to invoke the safe harbour remains, but this does not play out at the level of the definition of the hosting service. This is important considering the role of the hosting service definition in delineating online platforms and related **due diligence obligations**. A clarification that services should not lose their safe harbour as a result of voluntary measures with regard to illegal content and legal compliance with EU law is added to Article 6.

There are some remaining and new issues on these aspects of the proposal. The DSA proposal offers clarity with regard to the inclusion of social media and online marketplaces. I do not think that these two specific types of intermediaries each need a separate safe harbour provision so I support the proposal in this respect. Internet access provider activity is clearly covered by the mere conduit definition. However, **certain key online service providers that are important from the perspective of content moderation and illegal content online do not fit clearly into the three buckets for intermediary service activity** (mere conduit, caching or hosting) as defined. This is for instance the case for search engines, but there are other types of services for which the core service activity doesn't map easily onto the definitions of intermediary services. This creates uncertainty as to their legal liability, and the risk of continuing legal fragmentation as safe harbours for such services would end up developing at national level on the basis of general law. Notably, when a service does not qualify as an intermediary service as defined in the proposal, the due diligence requirements are (currently) not applicable either.

As mentioned, the **position of search engines and other information location tools in the DSA is not clear**. Search engines and their construction of an index and search results do not map easily to the definition of hosting service providers, as the construction of an index and search result pages do not clearly involve "the storage of information provided by, and at the request of, a recipient of the service". There are arguments for treating search engines (or similar) as caching services but, in the absence of a clear indication whether the legislator considers basic search engine activity to be covered by this definition, legal uncertainty will be considerable. Considering the scope of these services, EU level safe harbours are important for search engine operators, including smaller search engine operators in particular. Clarification is also needed as regards the applicable due diligence obligations for search engines. An easy solution would be to **stipulate that relevant parts of the due diligence obligations also apply to information location tools/search engines**. A more robust solution would be to create **clarity about the position of search engines in the basic definitions of intermediary services**, either by including them in an existing category or by including a separate definition of search engines as intermediary service providers.

There are **other services** in the internet service ecosystem for which the DSA proposal does not provide much clarity about their position. Recital 27 refers to services "establishing and facilitating the underlying logical architecture and proper functioning of the internet, including technical auxiliary functions", but dodges the question of whether such services (those mentioned are wireless local area networks, domain

name system (DNS) services, top-level domain name registries, certificate authorities that issue digital certificates, or content delivery networks) are within the scope of the proposal or not. **Further clarification in this area is required** and can help to provide overall clarity with regard to the scope of this legislation.

Another area in need of further clarification is **the status of (infrastructural) cloud services**, including basic infrastructural storage and computing services which underpin current day internet-based applications (including applications consisting of intermediary service activity themselves). Whereas traditional web hosting amounts to the storage of information to be made accessible to website visitors, cloud services make it possible to host complete services and applications for their end-users. Both types of activity involve storage of information and as such can be covered by the hosting definition as stipulated in the proposal. It would be helpful if the position of such services with regard to the hosting service definition is more explicitly clarified.

That still leaves the issue that some of the **due diligence obligations for hosting services are written with services in mind that are driving content moderation decisions** with regard to specific items of illegal content (instead of complaints about a website or a service). This is not a good fit for more infrastructural services whose policies and decision-making with regard to illegal content is significant but further removed from specific illegal content issues. **Clarification** of the way in which due diligence obligations apply to such infrastructural services is warranted.

As regards the definition of **online platforms and associated due diligence obligations**, the position of certain hosting services, including cloud services, should be clarified. In the case of a cloud service A that hosts an application B that involves the handling of user-generated content, the (new) requirement of **'dissemination to the public'** in the definition of online platforms, raises a set of new questions. Is this requirement meant to exclude service providers that are not directly consumer-facing in their (contractual) offerings? Taking the definition of 'dissemination to the public' literally, this appears not to be the case, as the cloud service is the one that makes the application available online for internet users. A problem here, however, is that it is **not clear who should be considered the recipients of the service**: the application providers contracting with the cloud service, the contributors to the application, or the general public accessing the application hosted on the cloud service? Considering the special nature of infrastructural services, this should be clarified. Such clarification of which group of platform users are to be considered recipients of the service is also important considering the definition of **very large online platforms** in Article 25(1).

Another notable element in the definition of online platforms is the requirement that dissemination takes place to "a potentially unlimited number of third parties". This requirement should also be seen in light of the complete exclusion from the scope of the DSA of **interpersonal communications services**, as defined in the Electronic Communications Code (Directive (EU) 2018/1972). Recital 17 of that Directive stipulates that *"Interpersonal communications services only cover communications between a finite, that is to say not potentially unlimited, number of natural persons, which is determined by the sender of the communication."* In reality, the distinction between interpersonal communications services and other social networking services is challenging. Many intermediary services provide users with significant control on how to use services, in particular whether the service is used with private restricted settings or used in ways that entail wider possible dissemination of content for other internet users.

Generally, I consider **the exclusion of interpersonal communications services from the scope of the DSA appropriate**. Private communications channels are subject to a different regulatory paradigm in relation to content, i.e. telecommunications regulation. At the same time, by excluding these services from the scope of the DSA completely, **they lose EU level clarification of their (limited) liability for the (potentially) illegal communications they facilitate**. If and when interpersonal communications services engage in some forms of **content moderation**, even if they facilitate communications between sender-determined finite numbers of users, I see no good reason to exclude them from the scope of the DSA. Finally, for very

large interpersonal communications service providers, there are questions as to which structural measures they can take, including design measures with regard to the onward sharing of private communications, that are relevant from the perspective of the DSA in protecting people in the online environment.

3. The DSA proposal and online advertising

Before discussing some issues with the proposed regulation of online ads, I would first like to make a note on the scope of the safe harbours as applied to sponsored communications. Currently, the proposal includes advertising networks and sponsored communication channels within the scope of the hosting safe harbour. This means that a service provider has the same limited liability for illegal content in sponsored communications (for which it receives direct payment, proportionate to increased dissemination), as for other user-generated content hosted and disseminated on the platform. In my view, such **limited liability should be reconsidered for sponsored communications that have a significant reach** on the relevant platform. In such cases, the platform is best positioned and can be considered to have sufficient financial means to make a meaningful assessment of any apparent illegality of the content of sponsored communications.

The DSA contains a number of specific **new provisions for online advertisement**. First, there is the requirement of advertising transparency for online platforms (excluding Small and Medium Sized Enterprises (SMEs)) in Article 24. Second, there is the obligation on Very Large Online Platforms (VLOPs) to provide for a publicly available ad repository in Article 30, as well as the obligation to consider advertising related risks in their systemic risk assessment (Article 26), and the consideration of risk mitigation measures by VLOPs that consist of the limitation of display of advertising.

With regard to Article 24, a first key issue is what can be expected from user-facing ad transparency measures and advertisement labelling. A recent study by leading researchers in the area calls for **caution against an overreliance on user-facing transparency solutions**². Without rigorous testing of specific disclosure methods, there is a risk that these new rules will not provide much benefit for (most) end-users.

Article 24 covers issues which are also within reach of data protection law (including ePrivacy), in particular the right to transparency about the processing of personal data and the requirement of a legal basis. The **DSA provides an opportunity to ensure more meaningful control of consumers over online advertising practices** in the context of online platforms, such as a robust right to opt-out of personalised advertising. When given a real choice, most users would prefer such tracking-free ads.

Advertising transparency (Article 24) runs into another challenge, which is that it applies only to sponsored communications for which direct payment was made by the sponsor of the message to the platform. Such sponsored communication exists alongside paid-for organic content creation and optimisation practices, which raises similar issues. So-called influencer marketing currently exists in a relative legal void (outside the audiovisual media context). The Parliament could **consider additional transparency requirements on influencer marketing and associated requirements on online platforms to ensure such transparency toward end-users**. Further, I would warn against the potential consequences of more stringent regulation of sponsored communication channels on opaque organic paid for content dynamics, including through influencers.

The **public ad repositories** required by Article 30 are an interesting new instrument and will create new forms of visibility and insight into the dynamics of advertising on online platforms, which would otherwise remain hidden in the interaction between services and individual users. The choice of requiring all advertising to be included is supported by the difficulty of separating different types of advertising

² Dobber et al. Effectiveness of Online Political Ad Disclosure Labels: Empirical Findings. 8 March 2021, https://www.uva-icds.net/wp-content/uploads/2021/03/Summary-transparency-disclosures-experiment_update.pdf

(commercial and political in particular) and the distinct benefits of transparency for political and commercial communications through VLOPs. Crucially, Article 30 lacks spending data, which is essential to make meaningful use of them. This omission is surprising as such information is included in existing ad libraries and is valued highly by researchers and journalists. I would therefore **strongly recommend including a requirement for spending data (how much money has been paid for the dissemination of each ad) in Article 30**. The obligation on VLOPs to consider **advertising-based business model** incentives in risk assessments is an important element, as the risks of the wrong incentives are considerable. I would recommend that further clarity is offered about the way in and the extent to which such risks are addressed by VLOPs.

As a final note, I would recommend that the legislator consider its assumptions about the ability and capacity of journalists, civil society and researchers to make use of the many new types of information that would become available and to create new forms of accountability on that basis. I would recommend that some forms of **independently structured funding opportunities for journalists, civil society and researchers, are created through the DSA that can help ensure that new forms of transparency in the DSA lead to meaningful accountability in practice**.

Brief Bio of the speaker, Prof. Joris van Hoboken:

Joris van Hoboken is Professor of Law at the Vrije Universiteit Brussels (VUB) and Associate Professor at the Institute for Information Law (IViR), University of Amsterdam. At the VUB, he is appointed to the Chair 'Fundamental Rights and Digital Transformation', established at the Interdisciplinary Research Group on Law Science Technology & Society (LSTS), with the support of Microsoft. He works on the protection of fundamental rights and the regulation of platforms and internet-based services.

Topic 2 of the DSA: Key Factors for an Effective Enforcement

(Prof. Teresa Rodriguez de las Heras Ballell, Carlos III University, Madrid)

1. Key Factors for Enhancing the Effectiveness of Enforcement: Analytical Framework

An effective enforcement system depends on a number of substantive, institutional, and procedural elements that interact with each other, that are interdependent of one another and that need to be consistently and adequately coordinated. To ensure the effectiveness of enforcement, all these elements need to be properly defined and must work in full coherence. In this regard, frictions, gaps, or inconsistencies among the components may undermine the effectiveness of enforcement.

Accordingly, **to assess the adequacy and the effectiveness of the DSA enforcement system, my proposal is that four tenets must be guaranteed:**

- (1) A clear and unambiguous (personal, territorial, objective) scope of application to ensure predictability for the providers regarding the applicable rules and to minimise the risk of circumvention of the law.
- (2) Well-defined obligations - extent, scope, conditions, and implications of infringements – to guarantee compliance and to increase legal certainty.
- (3) Effective remedies: proportionate, dissuasive, and easy to enforce.
- (4) Sound institutional and procedural mechanisms aimed to enhance coordination among authorities, to reduce costs and possible duplications, to streamline processes, and to ensure rapid and effective responses.

My assessment of the DSA's supervision and enforcement model will be then based on the above-described tenets, highlighting issues to consider and formulating recommendations.

2. A clear, predictable and unambiguous scope of application

If the scope of application of the DSA is not clear, legal certainty is compromised and the risk of circumvention of the law increases, which in turn means that the effectiveness of enforcement decreases. In assessing the scope of the DSA, three remarks have to be made:

(a) Limited definition of online platforms (Article 2(h))

Describing platforms as hosting services providers which merely store and disseminate information to the public is a definition that disregards the most distinctive features of platforms as self-regulated environments. Platforms create, regulate, and manage environments within which users interact with each other, negotiate, conclude, and even perform transactions (social networks, electronic marketplaces, sharing-economy platforms, etc.). Terms and conditions, internal rules and policies, procedures and mechanisms (as acknowledged by Article 12) lay down the framework within which users can carry out their activities and the provider (platform operator) regulates, supervises, enforces restrictions, moderates content, handles complaints, provides reputational mechanisms and recommender systems, solves disputes, etc.

Recommendations

- It would be advisable to **modify the definition of 'online platform'** to emphasise the key idea that platforms do not only store and disseminate information but they **provide for rules and policies aimed to govern and manage the activity** performed and content generated by users.
- **Definition of terms and conditions** (Article 2(q)) may be improved to highlight the fact that they are intended to **regulate not only the relationship between the provider and the recipient, but also, indirectly, the activity of the users in the platform**. Terms and conditions refer to and include by reference policies, internal rules, and community codes, the user accepts to abide by upon concluding the agreement with the provider (opening an account).

(b) Vagueness of 'ancillary' requirement

Insofar as the scope of application of the DSA is based on 'services' and not on 'providers', it is reasonable and possible to apply DSA provisions to certain services, even if they are ancillary to the main one (for instance, the comments section in a digital newspaper might be ancillary, but it may also represent a service with individuality and economic relevance). As determining the ancillary character will highly depend upon the business model and require a case-by-case analysis, it might in practice be uncertain and lead indeed to circumventing the applicability of the Regulation. A strategic interpretation of 'ancillary' may be a source of conflict.

Recommendation

- **Exclude that exception** or reformulate it to mitigate vagueness.

3. Know Your Business Customer – traceability of traders

Obligations have to be clearly defined to facilitate compliance and to ensure effective enforcement. The obligation Know Your Business Customer (KYBC), as laid down in Article 22, is going to be tested against such a benchmark. Some considerations aimed to improve enforcement and compliance are provided below:

General assessment: In my opinion, the policy underlying the KYBC duty is correct, clear, and is to be applauded. However, the formulation of the duty in the DSA may raise some uncertainties that can render compliance difficult and enforcement weak.

(a) Scope of the duty

- As the provision focuses exclusively on Business-to-Consumer (B2C) transactions, Peer-to-Peer (P2P) transactions seem to be excluded from the scope, as well as Business-to-Business (B2B) contracts.
- The duty is applicable to those platforms allowing users to conclude B2C contracts. The applicability may be put into question if traders only perform pre-contractual stages on the platform (advertising, offer, contact, comparison services, aggregation services, recommender systems directing consumers to other services, negotiation) whereas the contract is concluded outside of the platform.
- The current wording is not totally clear in determining who is responsible for verifying that the KYBC requirements indeed apply (B2C, contract conclusion, location of consumers in the EU). *Should the platform ask for self-assessment from each trader? Should the platform ensure that all requirements are met to apply the duty?* These questions are critical because, in case of non-compliance (incorrect information, non-provision, unverified data), the platform is entitled to suspend the provision of the services. Hence, clarity and certainty on the scope are critical to prevent unjustified restrictions on users' rights. *Is the refused trader entitled to*

object or complaint if the scope is not met, but the platform asks for reliable data, tries to verify, and suspends the service as per Article 22?

Recommendation

- It might be advisable to **clarify the policy underlying the determination of the scope and the resulting exclusions**. Drafting improvements might be required if the current outcome is not the desired one.

(b) Content and extent of the duty

Reasonable efforts: the rationale behind the policy decision to carve out the KYBC duty as a 'best-effort obligation' is realistic and pragmatic. Nonetheless, this also has an impact on the predictability of the compliance and the certainty in the enforcement. As explained below, the duty can be transformed into a mere 'checklist duty' with a formalistic character.

Verifying information and confirming reliability is costly. This may encourage platforms to implement procedures, protocols, and checklists as a pure formal compliance of the duty. Platforms can standardise collected data and evidence by designing interfaces and implementing checklists, and automate verification on the basis of formal protocols. It would transform the duty into a '*procedural compliance strategy*' based on developing compliant designs (as Article 22(7) seems to opt for).

The risk raised by a mere formal compliance is that it strongly depends on how much can be effectively automated. If information cannot be easily verified online through readily accessible official or reliable sources, costs increase and platforms do not have any incentive in facilitating the verification of traders. Therefore:

- Interoperable and fair access to registers and databases are needed in the EU, otherwise, an uneven playing field may be created between countries. In practice, effective and reliable verification depends on available information and accessible registers in each Member State.
- Possible discrimination of certain traders (individuals and SMEs) is likely if they are unable to provide reliable evidence and platforms tend not to accept it.
- Linguistic problems in the verification of information cannot be ignored, leading to different levels of verification efforts or success rates per country.
- Keeping data updated depends upon traders.
- Platforms might want to increase the rigorousness of the duty by determining the information to be provided, the evidence to submit, and the verification process in their terms and conditions. Is that an acceptable possibility?

Recommendations

- The availability of accessible reliable sources for platforms to verify on equal terms in the EU might reduce the risk of differentiated treatment. Member States might identify and list reliable sources for that purpose.
- Providing **guidance to platforms** on how to comply with the duty by elaborating guidelines, proposing standards, or promoting codes of conduct (Article 34).
- It might be advisable to clarify that **a trader rejected under Article 22 is entitled to lodge a complaint** both under Article 17(1)(b) and Article 43.

Liability of the platform as a Trusted Third Party: extent and implications. The most challenging issue arising from Article 22 is to determine the liability of the platform vis-à-vis the party who is relying on the trader's information: if the data are inaccurate, outdated, unverified, unverifiable, false. *Is the platform a Trusted Third Party?* More complex is the relation with Article 5(3): *if the information relating the transactions is presented in a way that it leads consumers to believe that information was provided by platforms or under their authority or control, besides excluding exemption of liability, might it render the platform liable for the information of the trader as well? Would the platform become the 'contracting party' (trader)? Might the consumer enforce contractual remedies against the platform?*

Recommendation

- **Clarifying platform's liability** under Article 22 and in connection with Article 5(3) is vital. Legal consequences of not complying with the self-certification as provided for by Article 22(1)(f) is not clear: neither traders' liability nor platforms' liability.

4. Algorithmic transparency and Artificial Intelligence

Definition of recommender system

With regard to recommender-system-related duties (Article 29) I want to stress three critical points:

- (i) including parameters in terms and conditions may in practice be ineffective;
- (ii) how options are offered to recipients in order to modify or influence is fundamental to make them effective and conscious; and
- (iii) options do not necessarily ensure understanding and explainability.

Recommendation

- It may be important to **stress that the aim of the recommender system is to recommend not only information by, in most cases and primarily, to recommend traders, content, products, offers, etc.**

Automation is explicitly mentioned or is impliedly referred to in several provisions, but legal effects are not specified.

Recommendation

The following **clarifications** should be considered in some provisions:

- Statement of reasons (Article 15): exclusively automated or assisted by?
- Complaint-handling (Article 17(5)): not solely taken on the basis of automated means, but to what extent can automated means be permitted? What does 'human intervention' mean? Is human review sufficient? When and how?
- Measures against misuse (Article 20): does "on a case-by-case basis" exclude any form of automation? Or, on the contrary, is automation allowed?
- Traceability of traders (Article 22): is the use of automated means for collecting, detecting errors, and/or verification permitted?

5. Enforcement

General critical assessment

The policy behind the designation of points of contact and legal representatives for the purposes of enforcement is laudable, but I find some difficulties and limitations in practice. In particular, there are doubts as to what necessary powers and resources to cooperate with authorities legal representatives should be

provided with. There is the risk of nominating a 'power-empty' legal representative. That renders ineffective the provision (Article 11(3)) providing for the liability of legal representatives for non-compliance. They could act as a mere 'front' in case of liability.

Country of origin (Article 40)

The jurisdiction-allocating solution is reasonable, but I do still find drawbacks. Jurisdictional arbitrage in deciding the place of establishment or the establishment of the legal representative is plausible. Disparity among Member States may exist. Hence, the risk of forum shopping by platforms is real.

Coordination

Relying on an enforcement system based on national authorities and direct enforcement powers for the Commission can benefit from the learned lessons in other areas, such as Competition Law. Procedural, practical, and substantive lessons can then be applied to ensure the effectiveness of the enforcement system. Alternatively, a bespoke agency to be created for the purposes of enforcing the DSA may reduce the Commission's workload, enhance specialization, and increase efficacy. Nonetheless, the creation of a new agency may be challenging due to the variety of legal issues to be tackled, and the horizontal approach of the DSA. Whereas the former model can more easily guarantee coherence and consistency in the decisions of the Commission in platform-related issues (*ratione materiae* and *ratione personae*), the latter one requires explicit coordination mechanisms. It should be guaranteed that, in case of a bespoke agency, the scope of application and powers are unambiguously demarcated.

A perfect and permanent coordination among Digital Services Coordinators (DSCs) from Member States is vital to ensure that the enforcement system succeeds. Each Member State needs to guarantee internal coordination by the DSC, but a clear attribution of competences to the DSC, *vis-à-vis* other existing authorities, may not always be clear. Overlaps with other general or sectoral legislation applicable to platforms may create duplication in enforcement (consumer rights, privacy and data protection, advertising). Member States may decide to create ad hoc DSCs.

Member States in designating their DSC must ensure that they have sufficient powers to enforce fines, penalty payments, cessation orders, interim measures (nature of the authority, applicable procedural rules) (Article 41(6)). *Are DSA rules sufficient to that end? Should Member States adopt detailed procedural rules to ensure the powers of the DSA?*

Orders under Article 8

Conflicting orders relating to illegal content among Member States is a possibility. In such cases, enforcement is complex and coordination becomes crucial. Multiple orders, especially if they are conflicting, undermine legal certainty. Besides, the effectiveness in enforcing orders within their territorial scope (Article 8(2)(b)) is a challenge.

Recommendation

- Redrafting of Article 52(4) is proposed. 'Lawyers duly authorised to act' is not a needed statement to be included in a Regulation. General agency rules and power of attorney standards should apply.

Brief Bio of the speaker, Prof. Teresa Rodriguez de las Heras Ballell:

Associate Professor of Commercial Law, Univ. Carlos III of Madrid, Spain. International Arbitrator. Member of the *EU Expert Group on Liability/Technologies formation* and of the *Expert Group to the EU Observatory on Platform Economy*. Expert at UNIDROIT and UNCITRAL in WG on Enforcement (Technology), Warehouse Receipts and Digital Economy (AI, Data transactions, Platforms). Spanish Delegate before UNCITRAL WG VI on Security Interests and WG IV on E-Commerce, and before UNIDROIT for MAC protocol. Member of the Inclusive Global Legal Innovation Platform (IGLIP) on Online Dispute Resolution (Gov Hong Kong – UNCITRAL).

1. US Developments in Platform Regulation

US intermediary liability law, which defines platforms' responsibilities for content posted by users, has three components. First, the Digital Millennium Copyright Act (DMCA) provides a detailed notice and takedown procedure, rather like the DSM Copyright Directive. Second, federal criminal law defines platform liability for worst-of-the-worst content like child sexual abuse material (CSAM) and terrorist content. Third, the law known as Communications Decency Act Section 230 (CDA 230) immunises platforms from state criminal law and a broad array of civil claims like defamation. It also protects platforms' decisions to remove users' speech under their own policies, immunising them from "must-carry" claims. Platforms have also successfully asserted a First Amendment editorial right to do so, regardless of CDA 230.

CDA 230's **"Good Samaritan" rule** expressly encourages content moderation. Its drafters envisioned a diverse array of competing services with different speech rules. Thus, platforms need not be neutral or passive to retain immunity, though they can't actively contribute to developing illegal content. They also, controversially, retain immunity even if they know about illegal content. This counter-intuitive standard reflects lawmakers' pragmatic calculation that platforms overall would be *more* likely to take action against illegal or harmful content if CDA 230 **protected them from the "moderator's dilemma"** – the fear that any effort to moderate user content would expose them to legal claims that they knew, should have known, or assumed editorial responsibility for users' unlawful posts. As I discussed in two [blog posts](#), this moderator's dilemma problem, which existed in pre-CDA 230 US law and exists now under the e-Commerce Directive, is difficult – perhaps impossible – to truly resolve without creating unintended and perhaps unjust outcomes.

CDA 230 has recently become very controversial in the US. It receives frequent, and often [inaccurate](#), attention from the press, lawmakers, and former President Trump – who vocally attacked CDA 230 throughout much of 2020. Then-candidate Biden said in one [interview](#) that he supported repealing the law, though Democrats now seem more inclined to amend it. Members of Congress introduced over twenty anti-230 [bills](#) in 2020, and eleven so far in 2021. Some can be seen as posturing or plays for media attention, and many are likely [unconstitutional](#). Others are seriously intended (these include, in my opinion, the [PACT](#) Act, [PADA](#), and [EARN IT](#).) All, however, face the same political bind: Democrats and Republicans have fundamentally different aims in amending the law. Broadly speaking, **Democrats often want platforms to take down more user content, while Republicans often want them to take down less**. These irreconcilable goals lead to a legislative stalemate for many proposals.

US lawmakers have fewer options for platform regulation than their EU counterparts for other reasons, too. The First Amendment poses a major barrier to many proposals, in both the "take down more" and "take down less" camps. Another barrier stems from a widely held reluctance to expand regulatory agencies. US legislators also have comparatively little experience with the "nuts and bolts" of content moderation, by contrast to European lawmakers who have gained great expertise over the past decade. US inexperience is not in itself a barrier to legislation, but does increase the risk that legislation will be poorly drafted. SESTA/FOSTA³, the 2018 amendment to CDA 230, is a case in point. It was intended to protect victims of sex trafficking, but has had major unintended consequences for the safety and societal participation of commercial sex workers. Lawmakers including Elizabeth Warren have backed a [bill](#) to assess the law's problems.

Given these barriers, **two kinds of legislation may stand the strongest chance of gaining traction in the US**. The first is legislation tackling harms so grievous that lawmakers on both sides of the aisle can find shared ground. This was the case with SESTA/FOSTA, as well as the 2020 EARN IT Act, a bill that was intended to

³ The Stop Enabling Sex Traffickers Act (SESTA) and Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) are the US Senate and House bills that as the FOSTA-SESTA package became law on April 11, 2018.

address CSAM, but was in my opinion quite [flawed](#). Alternately, lawmakers on the left and right might find common ground in a law that, like the EU's DSA or the US' PACT Act, focuses on *processes* for platforms' content moderation.

CDA 230 also continues to **evolve through new court cases defining the limits of platform immunities**. Importantly, one evolving area involves intermediaries that primarily facilitate transactions. Airbnb, for example, has been denied immunity from local laws regulating rentals – laws that in some senses resemble the register provisions of the DSA's Article 22. Amazon also continues to litigate its claimed immunity under CDA 230, and has lost important cases involving product liability claims under state tort laws.

I myself have [urged](#) US lawmakers to emulate the EU in several ways: by tackling privacy and competition in separate and robust laws, setting different standards based on intermediaries' size and technological function, and focusing on the real-world mechanics of content moderation. Perhaps with the current new administration, these approaches will become more feasible. In the meantime, the future evolution of CDA 230 remains unpredictable.

2. DSA Issues

As my US recommendations indicate, **I am broadly supportive of the DSA's legislative approach**. Still, I have some reservations. My remarks here will focus on issues affecting consumers and markets – though I believe that the fundamental rights issues raised by groups including Access Now, EDRI, CDT, and Article 19 also have real consequences for all of us in our capacity as consumers. My specific recommendations for amendments are tracked in a public (and evolving) online document, [here](#).

2.1. Preserve competition and innovative services by reducing burden on small platforms

The DSA inevitably requires complex **trade-offs between content regulation goals and competition and innovation goals**. Striking the wrong balance between those goals can further cement the dominance of current incumbent platforms – a consideration that may factor into those companies' legislative [advocacy](#). Setting vague legal standards rather than clearly defined obligations, as Article 12(2) appears to do, may create particular problems for smaller entities. In addition, the procedural protections for users that represent such a great step forward in regulating the largest platforms may present a serious barrier to entry for smaller start-ups and innovators. As currently drafted, for example, the DSA requires even the very smallest hosting platforms to issue detailed notices to users (Article 15). Those above micro and small enterprise scale must also track content moderation in sufficient detail to publish transparency reports (Art. 13), handle appeals (Article 17), and pay to engage with experimental out-of-court dispute settlement bodies (Article 18). The resulting operational and staffing expansion may exceed the capacities of many small platforms – giving companies with only tens or hundreds of employees responsibilities that incumbents like YouTube and Facebook did not encounter until their employees numbered in the tens of thousands.

I believe that **costs for smaller platforms should be proportionately reduced**. I cannot, as of now, confidently propose metrics defining which smaller entities should be so protected, but I believe that economists and others could devise them. And I feel confident in predicting that as currently drafted the DSA will deter innovators from investing their time and talent – and financiers from investing their money – in new platforms. If outside vendors arise to help meet DSA obligations, I would strongly expect them to contribute to simplification, technical stagnation, and lock-in of today's flawed approaches to content moderation.

2.2. Protect consumers from unintended harms

The DSA expressly protects consumers in a number of ways. Perhaps most prominently, **Article 22 adopts online marketplace rules that seem, to me, broadly sensible**. Articles 12-18 protect consumers against unfair treatment or exclusion from services, while also protecting fundamental rights such as freedom of

information. I believe these important provisions are well-drafted, though I do suggest some modest amendments. I particularly support **simplifying platforms' obligations with regard to the deceptive, high-volume commercial content commonly known as "spam"**. This term covers more than just junk email, including an array of content intended to manipulate and deceive both consumers and platforms themselves. Spams can represent a very high percentage of content moderation efforts – over 99% in Reddit's most recent [transparency report](#) – and they consume considerable resources. I believe that Articles 15-18 should be slightly amended to distinguish spam-fighting from other content moderation, in order to help platforms protect users without incurring substantial extra costs.

A second consumer protection issue implicated by the DSA is more fundamental. **The DSA should not undermine encryption**, the technology relied on by individuals, businesses, banks, and others as protection against hacking and invasions of privacy. In particular, it is not the place to entertain the controversial idea that technical "backdoors" can be created for law enforcement without fundamentally compromising consumers' protections from bad actors. Any change to the legal status of encryption would be highly consequential, and should be the product of very clear, careful, and informed debate – not an unconsidered result of ambiguous language in the DSA. I suggest amending Article 7 to address this issue.

2.3. Proceed with care in the DSA's most novel provisions

(a) Out-of-court dispute settlement

The **novel private dispute settlement mechanism of Article 18 should be deployed with care**, and closely monitored to understand its effectiveness and consequences. My tentative recommendation is that only VLOPs should be required to participate, and smaller platforms permitted to opt-in, at least for an initial period. Any extension to smaller platforms should take place only if real-world operations, costs and benefits, and areas for improvement are assessed.

(b) Regulating recommender systems

I am glad to see the DSA **proceeding with caution in approaching recommender systems**. I think that over the next few years we will develop much better understanding of regulatory options in approaching these systems. Allowing that public discussion to mature before enacting mandates other than these is, in my opinion, the wisest course.

3. Think holistically about transparency, and legislate accordingly

I am very excited by the DSA's broad transparency provisions – though must admit to some struggle in assembling the big picture from the many relevant provisions⁴. (And I am particularly curious about the seemingly very ambitious database proposed in Article 15(4).) Broadly, I have three recommendations in this area. The first and simplest is that **transparency requirements for platforms should be matched by obligations for high-volume notifiers and in particular for government actors**. The Parliament's draft of the Terrorist Content Regulation provides one possible model in this regard. The other recommendations are both more tentative. I believe both warrant additional – and prompt – discussion by civil society, academics, platforms, government actors, and other interested parties.

The second recommendation concerns **aggregate data disclosed in transparency reports**. As I recently [wrote](#), academics and civil society have a great opportunity to define their needs and seek relevant amendments. This requires a real effort to identify and prioritise the most useful information. At the same time, lawmakers should consider concerns raised by platforms, especially smaller ones, and deprioritise reporting if its burden outweighs its benefit. Evolving platform moderation practices make this exercise

⁴ Articles 13, 23, and 33 (content moderation transparency reports); 15 (Commission-maintained database of notices); 24 and 30 (ads); 29 (recommendations); and 31 (DSC and researcher disclosures). Additional data gathering may effectively be required as part of audits, risk assessments, and the like for VLOPs.

particularly difficult. It may make sense to set crisp rules and expectations for smaller platforms, and commit not to “move the goalposts” after they have already redesigned their data tracking tools, while at the same time allowing more flexible and evolving transparency requirements for the largest platforms.

The third recommendation involves **researcher access to content and other information not captured in transparency reports**. This is essential to identify problems platforms themselves are unaware of – like error rates or patterns of bias. I suggest modest amendments to Article 31 to improve such access, and to share findings with the public. Article 31 should also be carefully drafted to match research provisions of the General Data Protection Regulation (GDPR), and obviate unnecessary barriers – real or perceived – arising from that instrument.

Brief Bio of the speaker, Prof. Daphne Keller:

[Daphne Keller](#) directs the Program on Platform Regulation at Stanford’s Cyber Policy Center. Her [academic](#), [policy](#), and popular [press](#) writing focuses on platform regulation and Internet users' rights in the U.S., EU, and around the world. Until 2015, she was Associate General Counsel for Google, heading up work on web search and other areas.

Topic 1 of the DMA: Objectives, regulatory architecture and obligations

(Prof. Carmelo Cennamo, Copenhagen Business School)

The **DMA proposal seems to follow the logic of treating digital platforms as the “new utilities”** of the digital economy – i.e., digital infrastructures that need to guarantee equal access to and use of data and network resources. The concern is that the platform gatekeeper would use practices such as bundling and self-preferencing to favour its own services and limit innovation by business users that can challenge these services. This might eventually impair innovation around core platform services (CPS) and harm users. Thus, fairness and contestability are stated as the two main objectives of the proposal. However, there is no articulation about whether and how these objectives interrelate, and benefit consumers. Furthermore, innovation is never explicitly stated in the proposal as an objective, perhaps on the presumption that the incentives for innovation are best preserved in a fair and contestable market.

Platform gatekeepers do not just perform a “neutral” intermediary role: they create value primarily by continuously shaping the user interaction and consumption experience through technological and scope design choices that affect the direction of innovation for users in the whole ecosystem. **Digital platforms must be considered as new forms of “collective enterprise”⁵ in relation to the multi-actors and multi-products they coordinate** – they are new modes of organising economic activity. As orchestrators of the ecosystem, gatekeepers govern the interactions among different actors to provide direction for technology evolution and innovation, and curate a menu of value options for the consumer. In this sense, **the network and digital technology infrastructure are not neutral** to consumer choices: this curation and governance activity is central to the value creation process. This ecosystem view implies a potential reverse logic to follow in the regulatory architecture: to focus on promoting innovation (by business users, as well as by the gatekeeper) as a guiding principle to stimulate competition *between* ecosystems based on those distinctive features. This form of innovation-based competition can ultimately lead to greater contestability of core domains of platform gatekeepers. **The objectives and obligations of the DMA must be revisited considering this orchestration pivotal role** that platform gatekeepers play for innovation and value creation. This implies a different regulatory approach:

(Expected) consumer benefits → innovation → competition → (eventually) fairness

1. Objectives of the DMA

1.1. Include “promotion of innovation” as explicit objective

The DMA seems to put emphasis on the potential market failures (i.e., failures of “the proper functioning of the Single Market for digital services”) that may arise because of distortions instantiated by the gatekeeper for value capture interests (unfair practices protracted under limited market contestability). However, it misses to consider **innovation failures, or the problem of ecosystems not functioning properly in their capacity as organisational coordination tools for stimulating innovations** that need to come together to produce value and create specific value propositions for the consumer. In many cases, these failures emerge because of a lack of effective gatekeeping – or what is generally referred to in the literature as

⁵ See e.g. Jacobides, Cennamo and Gawer (2018), “Towards a theory of Ecosystems”, Strategic Management Journal - <https://doi.org/10.1002/smj.2904>.

“ecosystem orchestration”⁶. Such active control and coordination by the orchestrator are needed to shape innovation directions and align the incentives of external innovators accordingly.

This is “good” gatekeeping orchestration power - i.e., active regulatory control exercised by the gatekeeper to minimise innovation failure problems and free up value. While many can benefit from such orchestration power, some business users will be negatively affected. The issue is where do we draw the line between what is “good” and “bad” gatekeeping orchestration power - i.e., when this power is exercised to steer interactions in directions that allow the gatekeeper to capture greater value for itself while producing limited benefits (innovation spillovers) for others in the ecosystem. This is an area which we do not fully appreciate the consequences of yet, and the possible harms for (business and end) users. However, innovation cannot be treated as a secondary by-product that is consequential to fair trading in digital markets as presumed by the DMA – “[The proper functioning of the Single Market] *should* promote innovation”⁷ or “The benefits can be *expected to lead* to greater innovation potential amongst smaller businesses as well as improved quality of service, with associated increases in consumer welfare”⁸.

Experimentation of innovation related to product and services whose value relies increasingly on other interconnected products and services requires *shaping* (of vision and value propositions), *staging* (of interdependent processes) and *steering* (of activities) – a process being referred to as “market scaffolding”⁹. Without this coordination, systemic innovation in the ecosystem often fails. Stipulating the promotion of innovation as an explicit objective of the DMA would recognise the positive role of gatekeepers and direct their conduct towards this objective.

Recommendation

- **Include promotion of innovation by users in the ecosystem and by platform gatekeeper on CPS and technological features and ancillary services as a main objective of the DMA.**
- Practices listed under Articles 5(c), 5(f), 6(1)(a), 6(1)(c), 6(1)(f) are part of ecosystem orchestration core activities: they should not be banned when such practices are proved to **promote greater or higher-quality innovation or differentiated user experience across the ecosystem that benefit consumers.**

1.2. Clarify the concept of fairness

The fairness concept in the DMA seems to have a narrow focus that misses the implications for the rest of the ecosystem. For example, the possibility that the “unfair” practice is implemented to offer curated choices to end-users, or internalise possible negative externalities (e.g., free-riding problems in relation to excessive supply of lower quality offerings undercutting incentives of high-quality providers). Academic evidence shows that such orchestration can grow value for everybody in the ecosystem and lead to higher innovation activity (albeit in different directions)¹⁰.

⁶ See eg. Jacobides, Cennamo and Gawer (2018), “Towards a theory of Ecosystems”, Strategic Management Journal - <https://doi.org/10.1002/smj.2904>; Cennamo and Santaló (2019), “Generativity tension and value creation in platform ecosystems”, Organization Science - <https://doi.org/10.1287/orsc.2018.1270>.

⁷ DMA proposal, explanatory memorandum, p. 5 – emphasis added.

⁸ DMA proposal, legislative financial statement Proposal, p. 59 – emphasis added.

⁹ Cennamo, Constantiou and Wessel (2021). “The “love effect”: How platforms use selective promotions to create value” – Working paper.

¹⁰ See eg., Hagiu A. & Jullien B. (2011), “Why do intermediaries divert search?”, The Rand Journal of Economics, <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1756-2171.2011.00136.x>; and Foerderer J., Kude T., Mithas S., Heinzl A. (2018), “Does platform owner’s entry crowd out innovation? Evidence from Google Photos”, Information Systems Research, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2805510.

Recommendation

- **Include explicit accounting of value creation** i.e., a specific practice should be judged against its impact on the ecosystem (also on the “size of the pie” to be split not just who gets the “bigger slice”)

1.3. Clarify the concept of contestability

The contestability concept in the DMA seems to mainly refer to contestability *in* the market, narrowly defined as the CPS domain: this is too narrow a conceptualisation, which does not account for contestability that may proceed from competition *between* differentiated ecosystems. The whole concept of platform multisided markets is that the **kind of competition** that is relevant is not competition (between products) *in* a market but **competition for the market** (between alternative platform systems and between alternative market channels - including offline markets). It is this level of competition that the DMA should give primacy to *promote* contestability. The **level of competition** is also too narrowly restricted to the CPS. But that might not be the right level of analysis for platform competition. If one specific CPS is subject to tipping, which brings efficiencies and value for participants, forcing parcelling of this service into similar services would not restore or enhance vibrant platform competition. Platform competition does not come from standardisation but from *differentiation* of the core platform functionalities and consumer experience – that is, from the different way the ecosystem is orchestrated. Contestability of a platform’s dominance will likely not come from platforms operating similar CPS in similar ways, but from those offering a differentiated experience and service modality (e.g., consider Airbnb challenging Booking.com; or Amazon Alexa challenging Google Search; or Facebook-Shopify challenging Amazon Marketplace). Many of regulated individual CPSs, such as social media or online intermediation services, encompass a broader ecosystem of interconnected features that are part of one end-user experience. A too narrow focus on CPS might force an artificial segmentation of the competitive space, which might end up limiting contestability across platform domains.

Recommendations

- **Clarify that contestability includes competition for the market, that is between ecosystems, not just one-to-one competition to the CPS in the market, where the market is more broadly defined to include also adjacent related services and functionalities¹¹.**

- **Clarify how the Core Platform Service (CPS) definition applies to multi-sided or multi-product platforms,** which operate one main CPS whose features (e.g., marketplaces, communications services, search, etc.) might also individually qualify as separate CPSs. One option is to **broaden the definition of the CPS** to include also ancillary platform features and functionalities (such as e.g., user interface) that integrate with, extend, and enhance the same core platform service for end user experience.

- **Practices** by gatekeepers leveraging their CPS into related markets and domains should not be banned when such practices **promote greater platform competition (for the market)** across domains, and thus increase contestability of the dominant position of a gatekeeper in a domain.

2. Trade-offs

Possible trade-offs among the DMA objectives (and obligations) should be acknowledged and a rank-order principle should be established - e.g., when one practice might go against the fairness objective but promote increased competition and/or innovation, it should probably be allowed since it will produce a net positive. This has implications for competition policy analysis in the digital context: the **focus should be first on value creation** (how the target practice shapes the ability to produce new value from complementors

¹¹ A categorisation of three archetypes of digital platform markets is offered in Cennamo (2019) – core services might be organised within this broader market classification. Paper available at SSRN: <https://ssrn.com/abstract=3410982>.

(e.g. new complementary services/products that did not exist before) and expand the market set of consumption options). Analysis of value capture should then be subordinated to value creation.

Recommendations

- Make **"promotion of innovation" the guiding principle**, and subordinate the other objectives of contestability and fairness to it.
- Where complex trade-offs are involved, obligations should be included in Article 6 and subject to **case-by-case analysis and a regulatory dialogue**. This concerns all provisions relating to data, as well as the banning of self-preferencing or interoperability and neutrality mandates on a software service.

3. Obligations

Specific obligations should be reconsidered according to points 1 and 2. They should be **clustered coherently** according to the objectives they are supposed to achieve. Some require serious revisiting as they may be redundant, in conflict with one another or, worse, potentially not effective.

Article 5(a)

Consent-based data aggregation would add layers of friction and a breakdown of the user experience. It does little to promote any of the three different objectives detailed above. It might also impair the ability of small business users to innovate, causing unintended consequences like those produced by the compliance costs of GDPR¹².

Recommendation

*Clarify that the practice is banned when not directly linked to promoting innovation and user experience. Focus should be on ex-post possible **abuse/misuse of data**.*

Article 6(1)(a) and 6(1)(i)

These articles might be **in conflict or just redundant**. If a gatekeeper is obliged to grant the business user access to its own data, it will hardly breach the provision of Article 6(1)(a). Moreover, none of the data that are of relevant economic value for the user are "publicly available" – they are produced in the context of use in the platform. Granting unconditional access to data might also bring unintended negative consequences impairing innovation quality and competition – they might reduce control over quality and the ecosystem "curation" ability by the gatekeeper. These articles should be rewritten to strike balance between fairness and promoting greater choice for consumers and innovation.

Article 6(1)(d)

Consider **widening the scope** to include favourable treatment in ranking of services/products of any third-party unless it is clearly publicised to the end-user. Freedom of the gatekeeper to offer "curation" service and selective promotions (e.g., "apps of the month") should be retained.

Recommendation

"Self-preferencing" and third-party "preferencing" should be allowed when they are proved to enhance innovation (variety and/or quality) in the ecosystem, and/or help users discover new innovative services/products, and/or help differentiate the ecosystem and user experience compared to competing ecosystems.

¹² See e.g., Janssen R., Kesler R., Kummer M., Waldfogel J., "GDPR and the lost generation of innovative apps", http://conference.nber.org/conf_papers/f146409.pdf.

Article 6(1)(k)

Clarify what qualifies as “fair” and “non-discriminatory” general conditions of access to the gatekeeper’s software application store. Gatekeepers should be allowed to differentiate also based on the terms of access and engagement for ecosystem members – these are part of the design and governance choice.

Recommendation

Discriminatory conditions should be intended as specific restrictions or terms that apply to a specific business user and deviate from those that apply uniformly to any other business user in similar conditions.

Brief Bio of the speaker, Prof. Carmelo Cennamo:

Carmelo Cennamo is Professor of Strategy and Entrepreneurship at Copenhagen Business School, Affiliate Professor at SDA Bocconi School of Management, and Director of the [Digital Markets Competition Forum](#). His research focuses on competition in and between digital platform markets, and on business ecosystems.

Topic 2 of the DMA: Supervision and enforcement

(Prof. Heike Schweitzer, Humboldt-University, Berlin)

The extent to which the DMA will be able to achieve its goals to promote competition and ensure fairness will, to a significant extent, depend on an effective and timely implementation and enforcement. An effective and timely enforcement hinges on a number of aspects:

- The administrability of the legal rules
- Investigation and enforcement powers
- Possibilities for effective interim measures
- Sufficient resources available for enforcement

Effective enforcement is, however, not a goal in and of itself. Ultimately, it is the **sum of the error costs associated with a given set of rules and the costs of implementation and enforcement that should be reduced**¹³. In order to do so, the DMA proposal will still need some revision¹⁴. According to a widely shared perception, the DMA proposal currently leans towards a set of relatively concrete and uniform rules that may be **relatively cheap to enforce, but may tend towards over-regulation** that may sometimes even impede rather than promote competition; and at the same time may continue to produce “false negatives”.

This section focuses on the DMA’s supervision and enforcement regime, however, and recommends changes in three respects: (1) The market investigation regime; (2) Public and private enforcement; (3) Support infrastructure for providing technical information.

1. Market investigations

The DMA proposes to introduce market investigations as a new tool that shall support the implementation of the DMA (Article 15), its adaptation in case of changing market circumstances (Article 17) and the “escalation” of the regime in case of systematic non-compliance (Article 16).

1.1. Systematic non-compliance, Article 16

Article 16(1) provides the Commission with a possibility to impose “*any behavioural or structural remedies that are proportionate to the infringement committed and necessary to ensure compliance*” with the DMA where a gatekeeper has systematically infringed the Articles 5 and 6 obligations and has thereby further strengthened or extended its gatekeeper position. This is – or can become – a potentially important legal innovation, but it is in need of clarification. Currently, it teeters between a special sanctioning regime for repeat infringers and a mechanism that would allow the Commission to react when finding out that the list of obligations – and possibly behavioural remedies generally – do not suffice to react to the special features of digital markets and the market failures that result therefrom.

¹³ Christiansen / Kerber, Competition Policy with Optimally Differentiated Rules.

¹⁴ See Schweitzer, The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the digital Markets Act Proposal, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3837341.

Article 16 should clarify that it is meant to **enable to effectively address market failures that follow from the special features of digital markets where a systematic non-compliance suggests that the “normal” list of obligations, and possibly behavioural remedies generally, do not suffice**. Article 16 should not be designed as a sanctioning regime. The remedies imposed would therefore not need to be proportionate to the infringement, but they would rather need to be effective and proportionate with a view to the market failure addressed.

1.2. Empower the Commission to identify “core platform services” (CPS), Articles 10 and 17

Articles 10 and 17 of the DMA allow the Commission to close gaps in the lists of obligations in Articles 5 and 6. But when it comes to identifying new “core platform services”, the Commission can only propose to amend the Regulation. According to the current regime, new CPS can arguably be added to the list in Article 2(2) only based on a combination of a market investigation and a legislative procedure – which would amount to a very long process. Much argues for empowering the Commission to add new “core platform services” to the list where these display the special features characteristic for platform market and where a market investigation shows a tendency of the relevant markets to tip. Such an empowerment would need to be based on a general definition of “core platform services” in Article 2(2).

Recommendation

Empower the Commission to identify CPS, based on a general definition of CPS.

2.3. Add a new market investigation for tailored obligations

The goal of the Commission’s “New Competition Tool” initiative was to empower the Commission to ensure an effective protection of competition where competition law fails to do so, or to do so effectively. The scope of the market investigations proposed in the DMA is much more limited. In particular, what is currently absent is a possibility to impose tailored obligations on just one or a separate group of gatekeepers that create a specific danger to competition. Given the differences that may exist between different types of gatekeepers, such a possibility should be introduced.

Recommendation

Add a market investigation regime for imposing tailored obligations on specific gatekeepers.¹⁵

2. Centralised vs decentralised enforcement

2.1. Public enforcement

When it comes to the public enforcement of EU law, different models exist. **Normally, EU law is enforced decentrally by national agencies.** The competent authority is determined either by the country of origin principle (e.g. GDPR) or by the country of destination principle (e.g. consumer protection law). A sufficiently consistent application throughout the EU is ensured by the referral regime (Art. 267 TFEU). Sometimes, a special coordination regime is put into place in addition (e.g. Art. 60 GDPR). **Exceptionally, public enforcement is fully centralised.** The ECB’s competence for supervising systemically relevant banks is the best example. For the enforcement of EU competition law, the EU has opted for a third model, namely a **parallel enforcement at EU and national level**, combined with a coordination within the European Competition Network (ECN).

¹⁵ Such an instrument would help to close a gap that may remain between the draft DMA in its current version and competition rules. More particularly, it would help to address a situation in which Art. 102 TFEU proceedings might be too lengthy or ineffective in addressing the relevant problem. But at the same time, an updating of the lists of obligations under Art. 10 DMA is not advisable, because the obligation would be overbroad and costly when applied to all gatekeepers.

The DMA proposal opts for a **full centralisation of powers with the Commission** when it comes to the implementation of the new regime. The Commission has to designate the gatekeepers (Article 3), review the gatekeeper status (Article 4); decide on exceptional suspensions (Article 8) and exemptions (Article 9), on an updating of gatekeeper obligations (Article 10) or on a need for structural remedies due to systematic non-compliance (Article 16). Also, it is for the Commission to specify, based on a regulatory dialogue, the measures to be taken by the gatekeepers to fully and effectively comply with Article 6 (see Article 7(2)). In all these respects, a centralisation of powers with the Commission is needed to avoid a fragmentation of the internal market.

When it comes to the enforcement of the Articles 5 and 6 obligations, the Commission's enforcement activity (see Articles 25 and 26) will likewise be key. Given the EU-wide activity of the gatekeepers, the Commission will frequently be the natural enforcement authority in case of EU-wide and systematic infringements.

Nonetheless, the **DMA should allow for a parallel decentralised public enforcement** and thereby widen the role of national agencies which is currently very limited¹⁶. The nature of the obligations suggests that frequently, small and medium business users will be harmed. The number of complaints can quickly rise to significant levels. A backlog of complaints could absorb more resources than the Commission is able or willing to provide¹⁷ and could quickly endanger the core goal of the DMA to ensure quick interventions in cases of non-compliance.

In the field of **EU competition law, the transition towards a regime of decentralised enforcement with Regulation 1/2003¹⁸ has been a great success** – despite the broad and general nature of the relevant rules. **Cooperation** within the European Competition Network (ECN) ensures the necessary degree of consistency. A similar mechanism – including a regime of case allocation, information exchange and authority for the Commission to relieve a national authority of its competence at any point of time – will obviously be needed if a decentralised public enforcement of the DMA is introduced. At the same time, given the gatekeepers' EU-wide presence and business model, a decentralised public enforcement would need to imply an **empowerment of a national authority to take decisions of EU-wide application if the Commission does not step in**¹⁹. Article 60 of the GDPR can serve as a model in this regard. All in all, and given the European experience in other fields, a well-designed decentralised enforcement and networking approach should be considered a particular strength of the European model, not a weakness. In the EU – and contrary to the US model – national agencies can and should be integrated into the European endeavour, and not side-lined. Proposals to merely use national authorities as contact points for complainants, as monitors or as providers of input for a decision-making at the national level will fail to create incentives for national agencies to get engaged.²⁰

¹⁶ So far, NCAs can continue to apply Articles 101 and 102 TFEU (Article 1(6), 1st sentence DMA), they can apply their own national competition laws to gatekeepers (Article 1(6), 2nd sentence DMA), and three or more Member States can request the Commission to open a market investigation to designate a new gatekeeper, Article 33 DMA. In addition, the Member States are represented in the Digital Markets Advisory Board which shall facilitate an information exchange between the EU and the Member States.

¹⁷ See Commission, Explanatory Memorandum to the COM(2020) 842 final, DMA Proposal, 11: The Commission foresees a team of 80 Full Time Equivalents in 2025 for the DMA enforcement.

¹⁸ Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.

¹⁹ For a finding that the Commission's authority to specify measures that ensure effective compliance with Article 6 DMA (see Article 7(2) DMA) does not exclude a decentralised public enforcement. See Schweitzer, The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the Digital Markets Act Proposal, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3837341.

²⁰ For a recognition of the incentive problem see Monti, The Digital Markets Act – Institutional Design and Suggestions for Improvement, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3797730.

Empower national agencies to enforce Articles 5 and 6 of the DMA and provide for a cooperation regime between national agencies and the Commission.

2.2. Private enforcement

With many of the Articles 5 and 6 obligations (for example Article 5(a), Article 6(a) and Article 6(d)) compliance can be difficult to verify. An effective public enforcement will therefore be key. Other obligations, like Article 5(b), (c-g) and Article 6(1)(b), (c) or (e), may well lend themselves to private enforcement, however. The DMA proposal does not mention – and does not exclude – private enforcement. Under the current proposal, the “if” and “how” of private enforcement is left to the Member States. Arguably, EU law principle of effectiveness would *require* an effective private enforcement, however, as it does for the EU competition rules. In particular, business users of gatekeeper services should be able to sue for an injunction.

Recommendation

Introduce a **provision** into the DMA that **requires Member States to ensure that any business user who is harmed in its competitive opportunities by an infringement of the DMA is provided with an opportunity to sue for an injunction** in accordance with the principles of effectiveness and equivalence.

Brief Bio of the speaker, Prof. Heike Schweitzer:

Heike Schweitzer holds a chair for private law, economic law and competition law at the Humboldt-University, Berlin. From April 2018 – March 2019, Heike Schweitzer has acted as special advisor to Commissioner Vestager on future challenges of digitisation for competition policy. She also advised the German Economic Ministry on the reform of the regime of abuse control in the context of the 10th amendment to the German Competition Law.

Topic 3 of the DMA: The US perspective

(Prof. Fiona Scott Morton, Yale University)

1. The Position of the United States

Where is the United States when it comes to regulating big tech? Today, almost nowhere. **Digital platform regulation is not an idea that has gained any traction in the US. The first tool a US policy maker would try to use to combat market power is antitrust enforcement** because it is well-established under the law in the United States. However, for the last 40 years, antitrust law as interpreted by US courts has been moving backwards in the sense of getting farther from the economic literature and creating more burdens on plaintiffs. Public recognition of how far antitrust enforcement has strayed from its goal of protecting consumers and competition has been spurred by the unrestrained actions of large digital platforms. More recently, this recognition has become widespread among policy makers and academics. The House Majority Report on Big Tech released in October 2020 was important to changing public opinion²¹. Ten years after the EC first pursued Google under Article 102 (during which time there was almost no US digital antitrust enforcement), the dam finally broke: five big tech antitrust cases were brought by government enforcers between October and December of 2020. Both federal agencies and coalitions of state enforcers sued Google and Facebook for violating multiple antitrust laws.

At almost the same time, the Digital Markets Act proposal was released in the European Union. In addition, the US had a disputed election, a violent insurrection, and a large increase in Covid-19 cases. More recently, the presidential transition and vaccine rollout have also been distractions. The US policy community has therefore been focused on issues other than Big Tech and competition. In addition, antitrust and regulation get blended in people's minds and they think of them as all one issue – control of corporate power. They may therefore believe that the antitrust cases filed in 2020 will achieve a rapid and complete fix. However, the first hearing in the Department of Justice's Google Search case is scheduled for 2023, likely followed by an appeal and remedies phase. In addition, the idea that court-imposed remedies in particular cases will fix all the competition problems created by these digital platforms seems overly-optimistic, as the European experience shows²².

For these reasons, **the US is well behind the EU in regulating Big Tech**. The slow pace of antitrust enforcement, as well as the range of consumer protection and competition problems generated by digital platforms, indicate that attempting to rein in the market power of the largest platforms requires that regulation be part of the toolkit along with vigorous antitrust enforcement²³. Now, finally, the idea of regulating digital platforms is picking up steam and I expect to see a number of bills put forward by congressional representatives in the near future.

Because the EU has moved first with a draft law, and both bureaucrats and elected leaders have done some deep thinking about the way digital platform regulation should be carried out, there is a chance to be a global thought leader on this topic. Obviously, the more that regulation of digital platforms in the EU and the US are similar, the more the citizens of each can benefit from larger markets and the ensuing incentives to innovate and achieve economies of scale. Less conflict between legal regimes will benefit platforms, while cooperation among regulators will lower costs and raise expertise. The DMA states as its overarching goals

²¹ *Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations, Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, 116th Congress (2020).*

²² The Android and Shopping cases seem not to have increased competition in search.

²³ See e.g., George J. Stigler Center for the Study of the Economy and the State, *Committee for the Study of Digital Platforms Market Structure and Antitrust Subcommittee Report* (July 1, 2019), <https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report>; Digital Competition Expert Panel, *Unlocking digital competition* (Mar. 13, 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf; Jacques Crémer et al., *Competition policy for the digital era* (Apr. 4, 2019), <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>.

to promote contestability and fairness. **By explaining why the choices in the DMA limit market power and promotes these goals, the European Union has a chance to influence the way the rest of the world thinks about this regulation and the choices jurisdictions like the United States make.**

2. Underlying Principles of the DMA

Because the US follows a common law tradition, a US law typically articulates principles so that particular conduct can be assessed in light of those principles. Therefore, **an explanation of the relationship between the DMA's specific rules and its principles will help** policy makers in regimes where the legal system is different, but the same outcome is desired. Furthermore, the principles underlying the DMA are critical for guiding future expansion or modification of European regulations, which will be necessary given the fast pace of technological change in this sector. **There is a solid economic foundation for the underlying principles of contestability and fairness, and if these are stated they will help make the principles easier to understand and apply.** In addition, an economic foundation makes the DMA more accessible in the US where policy makers are accustomed to using economic analysis in regulation.

The DMA provides a number of criteria to identify what is called a gatekeeper platform. These criteria should include the concept of market power stemming from users who single-home. A core platform service (CPS) provided by a gatekeeper controls access to, or is the only practical cost-effective point of access to, a meaningfully large set of consumers on one side of the platform. The fact that the CPS's consumers single-home on the platform for a relevant need or opportunity affects entry and competition on the other side of the market. **Single-homing gives a CPS market power**, a traditional concept used in antitrust enforcement around the world, including the United States.

A key principle that is missing from the DMA proposal and is critical for both a US and an EU audience is the promotion of innovation. The digital sector generates significant valuable innovation that benefits consumers. Regulation is often blamed for stifling innovation, however, there are good reasons - which can be included in the law - to think the DMA will enhance, not harm, innovation. Since innovation is a dimension on which firms compete, **an increase in contestability will tend to increase innovation.** Spelling out more specifically how the DMA aims to foster innovation will help guide future revisions to the DMA and the specific solutions adopted to achieve effectiveness in implementation.

The economics of fairness:

A gatekeeper platform can retain the bulk of the surplus created by the joint activity of the platform and all its sides because of the imbalance in bargaining power between a platform and the members of those sides generated by network effects. Any individual consumer adds very little value at the margin. Similarly, one incremental complementary business adds very little value to the platform. As outside options are so important to bargaining over surplus, consumers and the businesses that operate complementary services on one side of a digital platform get a very small share of total surplus. However, if all users could move together to a similar competing platform, they would instead hold all the bargaining power because their collective contribution is very high. "Fairness" can be understood to consider a user's average contribution, rather than one user's marginal contribution.

The economics of contestability:

Contestability as it is used in the DMA measures the extent to which barriers to entry are low, entrants can enter, and competition (whether in the market, for the market, nascent, or potential) is strong. The EU can encourage the US to adopt a definition of contestability along these lines and repudiate the old and discredited economic model of the same name that was developed to protect the monopolist of that era,

AT&T (a telecommunications company – at that time, one of the largest corporations in the United States)²⁴.

The economics of user protection:

“User protection” combines together the regulations that protect end-users, as well as business user protection. User protection enhances contestability by creating transparency, preventing deception, and limiting harmful choice architecture, and in that way allows entrants to compete on a level playing field. Users will choose to move to a higher-quality provider when they can see and understand the quality they are receiving. But to take advantage of that understanding, there must be a competing choice to move to. User protection is therefore a complement to contestability. The EU is far ahead of the US on digital consumer protection, having rules on privacy, deception, basic standards for online selling, and so forth²⁵. However, the DMA includes several user protection obligations that are described as being only about business users. This seems like an unnecessary limitation. One can think about platform users along a continuum: from ordinary consumers who buy goods and services, to consumers who sell (a used handbag), to an artist selling jewellery made in the evenings after her regular job, to an artist who sells online as her regular job, to a business with 5 employees, to large corporations. All of these platform users will gain from protection from unfair or deceptive practices. In the future, the US is likely to adopt some form of digital user protection so that online markets function as well (or better) than offline markets. If the DMA explicitly includes effective user protection, this would be a helpful point of leadership.

3. Interoperability obligations

The DMA is missing a critical tool: interoperability. Interoperability is extremely powerful in lowering entry barriers and creating competition. It has the further advantage of requiring less intrusive oversight from a regulator. For these reasons, it may be the single most useful tool in the regulatory toolkit. Interoperability that is mandated or overseen by the government has a long history in modern economies. For example, physical telephone lines, modern wireless networks, and email are all interoperable (with different governance structures) so that competitive providers can serve interconnected consumers. Because modern programming is modular, a digital platform has many internal Application Programming Interfaces (APIs) that are used to pass data and instructions. When such an API is standardised and made public, outside entities are able to connect to the platform. When independent apps execute on a handset, they use such APIs – likewise when cross posting between two social networks, or when a home network connects to an appliance. Today in the US there is only one public bill of which I am aware that would assist in increasing competition in digital markets: the *ACCESS Act* sponsored by Senators Warner, Blumenthal, and Hawley in 2019²⁶. The bill allows the government to mandate interoperability in social media networks.

If one reads the DMA proposal, Articles 6(1)(c), (e), (f), and (h) carefully and thinks about the underlying principles, one can see that these rules are specific interoperability requirements. In that sense, the **interoperability tool is already part of the DMA – but not in a general enough way**. For example, the DMA proposal omits useful applications of interoperability: social networks, e-commerce marketplaces, and advertising technology to name a few. Because technology markets evolve quickly, a general rule requiring interoperability would allow the regulator to handle many more types of problems without needing to know

²⁴ In the US, the “contestability” theory argued that there would instantly be entry if a monopolist charged above the competitive price. This theory is completely discredited because it relies on unrealistic assumptions such as zero entry costs.

²⁵ See e.g., Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) OJ L 119/1; Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011, OJ L 304/64 (Consumer Rights Directive); Council Directive 2005/29/EC of 11 May 2005 amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No. 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive); Council Directive 93/13/EEC of 5 April 1993 (Unfair Contract Terms Directive).

²⁶ Augmenting Compatibility and Competition by Enabling Service Switching Act of 2019, S. 2658, 116th Congress (2019).

the specifics in advance. The DMA should add interoperability as an obligation under 6(1)(l) and require its use when that would increase contestability and fairness as the European Parliament called for in 2020²⁷. **An interoperability mandate must be paired with a non-discrimination requirement, so that platform functionality is the same for all parties.** By converting the CPS' bottleneck into an *interface* designed to promote entry and share network effects, contestability is enhanced. In addition, interoperability is likely to increase innovation. Access to the platform on the same terms as the platform's own services means a business user can invest securely and earn profit, and this will increase its incentive to innovate. Moreover, business user services are often geographically local to the consumers using them (e.g. a Dutch dating app) and so interoperability would likely increase EU-based innovation.

Interoperability will prove a powerful tool in combatting "tipping" in the Internet of Things and will complement Platform-to-Business Regulation. To achieve contestability, devices powered by dominant operating systems (such as refrigerators, cars, TVs, thermostats, road sensors) will have to be accessible by rival service providers. The operating system will likewise need to be interoperable so that rival device makers can connect and compete in those markets. Business users who innovate can take advantage of interoperability to attract end users who already own a device (for example, a TV) to their great new service, while businesses who invent a great new device will be able to sell it to end-users who can connect it to an existing network.

Interoperability can be implemented using the regulatory dialogue of Article 7. An interface such as between an operating system and an application, or a platform and a complement, should be chosen to: enable entry by rivals, make network effects occur at the market level rather than inside a proprietary CPS, and be non-discriminatory. These elements very likely require the input and oversight of the regulator to ensure effectiveness. Otherwise, an interface might not lower entry barriers in an important category or for an important type of entrant, or simply favour the platform. A dialogue with the regulator up front is critical.

4. Conceptual Clusters for DMA obligations

Rather than presenting the obligations as a list of rules, conceptually clustering them would allow policy makers in other jurisdictions to better understand the rules and be able to emulate them in their own environments. A list is difficult to map back to its underlying principles: one has no way to evaluate whether an item has been left off a list or an item has been included accidentally. **The principles of fairness, contestability, and user protection might be a helpful way conceptually to organise the obligations** and make them more understandable to readers in other countries. The 18 specific rules of the DMA fall into three groups according to these principles. Existing interoperability provisions are listed in [blue](#) below and the proposed new interoperability provision is listed in [red](#).

User Protection: full information is provided to users, full consent is obtained from users, and users have the freedom to not use specific services.

- No data fusion without user consent - Article 5(a)
- No prevention of complaining - Article 5(d)
- No requirement that business users use the identification service of the platform to use CPS - Article 5(e)
- Ad price transparency - Article 5(g)
- Allow un-installing of apps, unless essential to OS/device - Article 6(1)(b)

²⁷ This has already been recognised as such by the European Parliament in its October 2020 resolution, paragraph 81: "Underlines that interoperability is key to enable competitive market, as well as users' choice and innovative services, and to limit the risk of users' and consumers' lock-in effect; calls on the Commission to ensure appropriate levels of interoperability for systemic operators and to explore different technologies and open standards and protocols, including the possibility of a technical interface (Application Programming Interface);"

- Ad performance transparency - Article 6(1)(g)

Contestability: businesses may directly connect to users on better terms without the CPS, tying and leveraging by the CPS is prohibited, **interoperability is required.**

- No Most Favoured Nation (MFN)/price parity clauses - Article 5(b)
- No type of end-user must subscribe or register with one CPS in order to use another - Article 5(f)
- **Allow side-loading of 3rd party apps and app stores, unless it threatens integrity - Article 6(1)(c)**
- No self-preferencing in rankings - Article 6(1)(d)
- **No technical restriction of switching or multihoming across apps using OS - Article 6(1)(e)**
- **Access to proprietary OS equivalent to owner - Article 6(1)(f)**
- **Provide real-time data portability - Article 6(1)(h)**
- Fair, Reasonable and Non-Discriminatory (FRAND) access to search data - Article 6(1)(j)
- **Provide non-discriminatory interoperability at bottleneck points - proposed Article 6(1)(l)**

Fairness: disintermediation to avoid the gatekeeper's fees is allowed, users have full use of own data, a CPS must charge a fair price for access.

- No anti-steering rules to keep users on the platform; no prohibition of disintermediation - Article 5(c)
- No use of non-public data generated by the activity of business users to compete against those business users - Article 6(1)(a)
- Obligation to share real-time data generated through activity of business users with business, for free, with consumer consent - Article 6(1)(i)
- FRAND access to app stores - Article 6(1)(k)

Brief Bio of the speaker, Prof. Fiona Scott Morton:

Fiona Scott Morton is the Theodore Nierenberg Professor of Economics at the Yale School of Management. Her research is in the area of industrial organization (the study of firms, markets, and competition), and she is widely published both in economics and law journals. She served as chief economist at the Antitrust Division of the US Department of Justice under President Obama.