CPI COMPETITION POLICY® INTERNATIONAL

Competition Policy International, a What's Next Media and Analytics Company

LETTER FROM THE EDITOR

Dear Readers,

This edition of the Chronicle examines upcoming changes in EU platform regulation. Specifically, it focuses on the EU Digital Services Act ("DSA") from a competition perspective. The DSA is perhaps little understood compared to its companion regulation: the Digital Markets Act ("DMA"), which explicitly aims to increase the contestability of digital markets. But the DSA, particularly via its modification of liability rules for platforms, will also have competitive effects on digital platforms.

The DSA sets itself the laudable aim of ensuring a "safe, predictable and trusted online environment" by targeting various forms of harmful behaviors online, including the spread of illegal and harmful content, such as disinformation. Indeed, the DSA is remarkable in its ambition, as noted by **Michèle Ledger & Laura Sboarina**. The DSA explicitly seeks to make the internet a "safer place," while also seeking to protect fundamental rights and enhance consumer protection. This new regulatory framework places important responsibilities on intermediary services, depending on their reach and size relating to the moderation of content. **Julia Apostle, Kelly Hagedorn, Christian Schroder & Adele Harrison** further detail the obligations imposed by the DSA. Despite the DSA coming into force in February 2023, many businesses do not know yet that are subject to the DSA. The authors provide an overview of the DSA, including its scope of application, key obligations, when they take effect, and sanctions for violations.

It also covers other aspects of digital services, such as exploitative online advertising and "dark patterns," including manipulative and coercive user interface designs. That said, the DSA does not address the moderation of media services (but this is now covered in the Commission's proposed European Media Freedom Act). The authors query whether the DSA will deliver on its promise, or whether it is too ambitious.

Turning to more concrete aspects of the changes to the rules governing platforms, **Maciej Sobolewski & Néstor Duch-Brown** argue that the DSA, via the modification of liability rules for platforms, could also bring about competitive effects in the platform economy. The authors, after setting out the case for reform, conjecture as to how platforms might adapt to the new rules. Finally, they hypothesize as to how the DSA might affect competition between large and small platforms via changes in content curation behavior.

Delving further into the detail, **Katie Pentney** explores the particular due diligence obligations the DSA places on large online platforms, like Facebook and Twitter, to achieve its ends. As the author notes, the vagueness of the provisions, the deference afforded to these platforms, and the disjointed approach to harmful content such as disinformation may hamper the DSA's ability to fulfil its promise. This article sets out the key provisions of the heightened due diligence framework, the underlying compromises made during the negotiations, and the lingering challenges that lie ahead.

Taking yet a further deep cut, **Oliver Budzinski & Madlen Karg** discuss how the DSA will interact with algorithmic search and recommender systems. Such systems have the key function of pre-sorting the torrent of online information for users' benefit. However, they also harbor the risk of competitive distortions and, perhaps more controversially, alleged ideological bias.

The DSA responds to this concern primarily through the imposition of transparency obligations, which the authors analyze from a law and economics perspective. Contrary to the DSA's vaunted aims, the authors conclude that the proposed approach neither prevents possible distortions of competition nor ideological media bias. Therefore, according to the authors, there is a risk that the DSA´s transparency requirements will become a paper tiger.

These debates will no doubt continue to rage as the DSA is implemented (along with the DMA, its partner regulation). At this formative time in the development of online media regulation, the pieces in this Chronicle set the stage for the controversies to come, with a particular focus on their potential effects on competition.

As always, many thanks to our great panel of authors.

Sincerely,
CPI Team

TABLE OF CONTENTS

CPI COMPETITION POLICY® INTERNATIONAL

DIGITAL SERVICES ACT

DECEMBER 2022

SUMMARIES

THE DIGITAL SERVICES ACT – A LAUDABLE AMBITION, BUT WILL IT DELIVER?

By Michèle Ledger & Laura Sboarina

The EU has adopted the Digital Services Act ("DSA") a ground-breaking legislation to make the internet a safer place, while also seeking to protect fundamental rights and to enhance consumer protection. This horizontal framework places important responsibilities on intermediary services, depending on their reach and size relating to the moderation of content. Other – more surprising aspects – are also covered such as online advertising and dark patterns, while the moderation of media services is not addressed (but is now covered in the Commission's European Media Freedom Act). The DSA places a large emphasis on oversight and enforcement but will the DSA deliver or is it too ambitious?

YOU MAY BE SUBJECT AS WELL!: DIGITAL SERVICES ACT – WHAT COMPANIES NEED TO KNOW

By Julia Apostle, Kelly Hagedorn, Christian Schroder & Adele Harrison

The EU Digital Services Act ("DSA") is in force and the first of its requirements will soon take effect. And yet, many businesses do not even know yet that they are subject to the DSA. The landmark legislation DSA has a large scope of application, covering a significant range of online services that target EU users. In particular, companies that make available to the public any third-party content, whether B2B or individual user content, may be subject to its rules. This article provides an overview of the DSA, including its scope of application, key obligations and when these take effect, and sanctions for violations. It will also identify some of the steps that organisations should be taking now to achieve compliance.

CONTENT MODERATION AND COMPETITION IN DIGITAL MARKETS

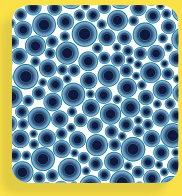
By Maciej Sobolewski & Néstor Duch-Brown

In this contribution we look at the upcoming changes in the EU platform regulation. More specifically, we focus on the Digital Services Act ("DSA") from the competition perspective. The DSA is less frequently discussed from this perspective compared to its companion regulation: the Digital Markets Act ("DMA"), which explicitly aims to increase contestability of digital markets. We argue that the DSA, via the modification of liability rules for the platforms, may also bring competitive effects to the platform economy. To set the scene we discuss why an update of liability regime was necessary in the first place. Then we conjecture how platforms may adapt to the new rules and argue that more content screening can be expected. Finally, we hypothesize how the DSA may affect competition between large and small platforms via changes in content curation behavior. We sketch conditions under which the existing differences in size between the platforms could decrease leading to a more balanced market landscape.

OPERATIONALIZING THE REGULATION OF ONLINE CONTENT UNDER A DEMOCRATIC DEFICIT: THE DIGITAL SERVICES ACT

By Dr. Joseph Downing

Europe is currently experiencing a renewed raft of social media regulations with the newly adopt Digital Services Act. This is significant because it demonstrates the European Union further intervening into the technology and digital arena. This Europeanisation of digital services legislation is muscular and sets out significant provisions for social media companies to be sanctioned for non-compliance and presents a range of issues for social media companies. In addition, the measures are unlikely to be a "silver bullet" solution to the range of problems presented by social media platforms. This intervention comes within a European context where American big tech has been blamed for many contemporary political and social ills, including fueling the rise of extremist politics and spreading disinformation in the context of the COVID-19 pandemic.



THE DSA, DUE DILIGENCE & DISINFORMATION: A DISJOINTED APPROACH OR A RISKY COMPROMISE?

By Katie Pentney

The newly-introduced Digital Services Act ("DSA") sets as its ambition ensuring a "safe, predictable and trusted online environment" by targeting the spread of illegal content, on the one hand, and the spread of harmful content, like disinformation, on the other. It imposes particular due diligence obligations on very large online platforms, like Facebook and Twitter, to achieve this end. But the vagueness of the provisions, the deference afforded to these platforms, and the disjointed approach to harmful content like disinformation specifically may hamper the DSA's ability to fulfil its promise. This article sets out the key provisions of the heightened due diligence framework, the underlying compromises made during the negotiations, and the lingering challenges that lie ahead, particularly with a new leader – and self-proclaimed "free speech absolutist" – at the helm of Twitter.

ALGORITHMIC SEARCH AND RECOMMENDER SYSTEMS IN THE DIGITAL SERVICES ACT

By Oliver Budzinski & Madlen Karg

It is impossible to imagine digital services without algorithmic search and recommender systems. They have the important function of pre-sorting the flood of information online for users. However, they also harbor the risk of competitive distortions and ideological bias. At the European level, the Digital Services Act responds to this primarily with transparency obligations, which we analyze in this article from a law and economics perspective. We conclude that the approach neither prevents possible distortions of competition nor ideological media bias. Therefore, there is a risk that the DSA´s transparency requirements will remain a paper tiger.


BRAVO!

THE DIGITAL SERVICES ACT – A LAUDABLE AMBITION, BUT WILL IT DELIVER?

BY MICHÈLE LEDGER

& LAURA SBOARINA

Respectively, Head of Practice - Cullen International, Researcher and Lecturer at CRIDS/NADI - University of Namur, Research Fellow – CERRE; and Principal Analyst - Cullen International.

01 INTRODUCTION

The Regulation on a Single Market for Digital Services and amending Directive 2000/31/EC, nicknamed the Digital Services Act ("DSA") was finally adopted on 4 October 2022, less than two years after it was first proposed by the European Commission. It was published in the Official Journal on October 27, 2022 and while some of its provisions will apply earlier, it will be directly applicable in the 27 Member States on February 17, 2024.[2]

2 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065&from=EN.

The DSA is a horizontal instrument introducing different tiers of obligations to be applied by online intermediaries (depending on their reach) to counter the dissemination of illegal and harmful content while also seeking to protect freedom of expression. At the same time, the DSA also introduces rules to protect users against misleading online advertising, recommender systems and so-called dark patterns. It carries over the rules on the liability of intermediaries that are contained in the Electronic Commerce Directive[3] without changing these rules very substantially.

This article explores some of the most striking aspects of the new regulation, linked to the fact primarily that the DSA is a horizontal legal framework. It focuses on its (very broad) scope, the obligations to deal with illegal and harmful content, the safeguards against arbitrary content moderation (including of media services), and some of the enforcement and oversight aspects of the new regulation.

02
SERVICES IN SCOPE

The DSA applies to an extraordinary wide range of online services.[4] These are intermediary services defined[5] as a sub-set of information society services[6] i.e. mere conduit, caching and hosting services which were hitherto also defined and regulated under the Electronic Commerce Directive.[7] The DSA in fact repeals the references in the Electronic Commerce Directive to these services and to the rules on liability for third party illegal content and re-introduces them (with some clarifications) in the DSA.

Mere conduit and caching services are the technical internet layer and cover services such as internet access services, electronic transmission services and proxy servers.[8]

It is quite surprising that these services are covered because none of the other legal instruments that have introduced responsibilities on online intermediaries have so far targeted the technical layer. It would seem that these intermediaries are covered primarily because the DSA is now the home of the rules on the liability of intermediaries which also cover these technical intermediaries. This may create a number of difficulties since these intermediaries are also regulated under the European Electronic Communications Code[9] and are hence under the oversight of the national regulatory authorities ("NRAs") in charge of electronic communications services, whereas the DSA introduces a new layer of supervision of these intermediary services as explained below.

Hosting services cover for instance (on top of online platforms defined as explained below) cloud computing and webhosting services.

The DSA places more responsibilities on online platforms – a subcategory of hosting services – that at the request of a recipient of the service, store and disseminate information to the public (a potentially unlimited number of third parties) unless that activity is a minor or purely ancillary feature of another service.[10] This is potentially the largest category since it covers social media platforms, video-sharing services, app stores, marketplaces but also the travel, transport and accommodation services platforms to the extent

3 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ((OJ L 178, 17.7.2000, p. 1).

4 M. LEDGER, S. BROUGHTON MICOVA, Overlaps - services and harms in scope : comparison between recent initiatives targeting digital services, Bruxelles, CERRE, 2022, 52 p.

5 Article 3 (g) of the DSA.

6 Information society services are defined in Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

7 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ((OJ L 178, 17.7.2000, p. 1).

8 Schwemer, S., Mahler, T. & Styri, H. (2020). Legal analysis of the intermediary service providers of non-hosting nature. Final report prepared for European Commission.

9 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

10 Article 3 (i) of the DSA.

of course that they qualify as information society services.[11] Further obligations are also placed on online marketplaces and other platforms that allow consumers to conclude distance contracts with traders. [12]

Despite not having been initially specifically covered by the proposal, online search engines are now clearly in scope. They are defined as a special type of intermediary service[13] but except for paid for (or sponsored) search results, which are – in line with the case law of the Court of Justice of the EU – considered as hosting services, it is not clear if natural or organic search results will be categorised as caching or hosting services. This may have legal consequences as the duties for caching and hosting services are not identical.

> ***Despite not having been initially specifically covered by the proposal, online search engines are now clearly in scope***

Then the largest responsibilities are placed on the very large online platforms ("VLOPS") and search engines ("VLOSES").[14] These are the platforms or search engines that have at least 45m active recipients in the EU on a monthly basis. This represents around 10 percent of the EU's population. The VLOPS and VLOSES will be designated by the Commission and their names will be published in the Official Journal.

Lastly, like many of the more recent EU legislations, intermediaries that do not have an establishment in the EU will be covered if they have a substantial connection with the EU. This could be deemed to exist if they have a significant number of recipients in one or more Member States in relation to the population, or if the service provider targets its activities towards one or more Member States as evidence by relevant circumstances such as language or currency. [15]

The DSA also foresees waivers from certain of the obligations for micro and small enterprises.

This extremely wide scope of application may cause practical difficulties. Indeed, no mechanism is foreseen in practice on the designation process of the intermediaries in scope, except as explained above for the VLOPS and VLOSES which will need to be designated by the European Commission. Some Member States may therefore launch studies to understand which services they will need to regulate, while others may want to introduce a self-declaration or notification requirement of the intermediaries established in their countries.

03
HARMS IN SCOPE

The DSA also has an extraordinary wide scope of application in terms of the harms in scope. It deals primarily with countering the dissemination of illegal content, which is defined in a very broad manner.[16] First, it covers information irrespective of its form: content, products, services or activities are all in scope. Then, illegality is defined by reference to what is not in compliance with Union law, or the law of any Member State, provided that national law is in compliance with Union law, irrespective of the precise subject matter or nature of the law.

It is therefore striking to note that, except for some caveats explained below, all breaches of law are treated in the same manner. A breach of consumer protection legislation will be treated in the same manner as a conduct that constitutes a criminal offence. This may lead platforms to be flooded with requests to remove content considered to be illegal on "trivial grounds," leading perhaps to delays in the processing of the serious requests. We note for instance that the UK's Online Safety Bill[17] which is being discussed in the UK Parliament introduces a tiered approach, since

11 See in particular Case C390/18 *Airbnb Ireland UC v. Hotelière Turenne SAS,* [2019], Case C- 434/15 *Elite Taxi v. Uber Systems Spain SL,* [2017], Case C62/19 *Star Taxi App SRL v. Unitatea Administrativ Teritorială Municipiul Bucureşti prin Primar General and Consiliul General al Municipiului Bucureşti,* [2020].

12 These rules are detailed in Section 4 of the DSA.

13 Article 3 (j) of DSA.

14 These rules are detailed in Section 5 of the DSA.

15 Article 3 (d) (e) of the DSA.

16 Article 3 (h) of the DSA.

17 https://bills.parliament.uk/bills/3137.

it lists "priority offences" which platforms need to remove with priority.

The second element that appears surprising is that there is no real mechanism to help intermediaries determine if the national legislation that is alleged to be breached is in line with Union law, which includes of course the EU Charter on fundamental rights. Does the platform need ipso facto to examine this (in)compatibility or does the (in)compatibility need to be raised by the person's whose[18] content could be removed? In addition, deciding on the (in)compatibility may require a complex legal analysis, which may not be able to be carried out by the platform itself.

That being said, it may also be noted that the DSA also covers the category of "manifestly illegal content" but only defines this category, by saying that this is where it is evident to a layperson, without any substantive analysis that the content is illegal.[19] In relation to this type of content, as explained below, online platforms are required to suspend accounts in relation to users that frequently post such content. It also obliges hosting services to notify to law enforcement or judicial authorities any suspicions that a criminal offence, involving a threat to life or safety has oris taking place or is likely to take place.[20]

Harmful content is dealt with in the DSA but in an indirect manner as explained below. In any event, the co-legislators have been careful not to define this notion, unlike in the UK's Online Safety Bill.

> ***Harmful content is dealt with in the DSA but in an indirect manner as explained below***

It must be noted that more focussed legislation exists in the EU to either set more detailed obligations in relation to certain specific harms such as terrorist content[21] or in relation to specific types of online intermediaries such as video-sharing platforms,[22] or both. For instance, the Directive on Copyright and the Digital Single Market deals with online content sharing platforms and their duties in relation to the clearance of copyright uploaded by the users of the platforms.[23] Legislation to tackle the dissemination of child sexual abuse and grooming is also in the process of adoption.[24]

04

OBLIGATIONS TO DEAL WITH ILLEGAL CONTENT

The DSA does not introduce a requirement for platforms to filter illegal content before it is uploaded by their users as this would disproportionately limit users' freedom of expression and freedom to receive information.[25] Instead, it requires all platforms (except the technical internet intermediaries) to operate a notice-and-action procedure whereby platforms must deal with illegal content when users send notifications and (depending on the type of platform) take additional measures for content that is "manifestly illegal." Also, VLOPS and VLOSEs must conduct an annual risk assessment of how their service contributes to the dissemination of illegal content and take the appropriate measures of their choice to mitigate the risks identified. Additional specific provisions apply to online marketplaces with the purpose of fighting fraudulent practices and the sale of illegal products.

18 https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html.

19 Recital 63 of the DSA.

20 Article 18 of the DSA.

21 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of the terrorist content online (OJ L 172, 17.5.2021, p. 79)

22 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (OJ L 95, 15.4.2010, p. 1).

23 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92).

24 Proposal for regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, 2022:0155(COD), 11.5.2022, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN.

25 Article 8 of the DSA prohibits member states (as in Art. 15 the 2000/31/EC E-Commerce Directive, now deleted) to impose a general obligation on information society services to monitor the information or to actively seek illegal information.

The notice-and-action procedure must comply with a set of obligations. The most interesting one is that the DSA specifies the elements that need to be contained in the notices (e.g. exact location and grounds for considering the content illegal.)[26]

It must be noted that when the notice is accurate, the platform will be presumed to have actual knowledge and could therefore risk incurring liability but only where a diligent provider would be able to determine the illegality of the notified content "without a detailed legal examination." Fundamental rights associations have welcomed this clarification introduced by co-legislators because otherwise platforms would be "inappropriately required to make determinations on the illegality of content" and incentivised to "remove any content notified to them," beyond content that is "evidently manifestly illegal." [27]

Platforms are required to process (including automatically) any notice they receive through this system, and to take "timely" decisions about it. However, online platforms (i.e. not the technical hosting services) must immediately act (or decide not to act) when they receive notices from so-called "trusted flaggers."[28] These are (public or non-governmental) entities with proven expertise and independence from platforms that will be designated by the relevant Digital Service Coordinator ("DSC") that will need to be designated by the Member States as explained below.

In all cases, platforms must inform flaggers of the decision taken and of the possibility to complain. To avoid misuses, the regulation requires online platforms to suspend users that frequently submit manifestly unfounded notices.

As mentioned above, platforms must take further measures to deal with content that is manifestly illegal (e.g. criminal offences). In particular, all platforms (including technical hosting service providers) need to immediately report to the relevant law enforcement or judicial authority any suspicion of a criminal offence that has or is threatening someone's life or safety (or is likely to do so), such as child sexual abuse.[29]

Online platforms must also temporarily suspend the service for users that frequently provide any content that is manifestly illegal (irrespective of how they get aware of it).[30]Interestingly, the DSA does not provide any details as to the meaning of what constitutes a frequent infringement or the length of the required suspension. However, it specifically requires online platforms to specify in T&Cs their policies regarding frequent infringers with examples of conducts and length of suspensions. In any event, before suspending the provision of the service, they would need to send a prior and detailed warnings to the users concerned.[31]

The regulation accurately details how the VLOPS and VLOSES must undertake the annual assessment of the risk of dissemination of illegal content but interestingly it does not provide criteria to define when the results of the assessment require action.[32] Also, the choice of the specific measure remains with the provider. Only a recital clarifies that the relevant risk might be identified when access to illegal content spreads rapidly and widely through accounts with a particular wide reach or other means of amplification.[33] One of the mitigation measures mentioned in the DSA that seems relevant in this regard is adapting the speed and quality of processing notices related to specific types of illegal content.

That said, the Commission can adopt guidelines to present best practices and recommend possible measures.

26 Art. 16 of the DSA.

27 Centre for Democracy and Technology "A series on the EU Digital services Act"

28 Art.22 of the DSA.

29 Art.18 of the DSA.

30 Art.23 of the DSA.

31 Article 24.4 of the DSA.

32 Arts 34 and 35 of the DSA.

33 Recital 80 of the DSA.

05
OBLIGATIONS TO DEAL WITH HARMFUL CONTENT

On top of rules to fight the dissemination of illegal content, the regulation includes some provisions to address content that is harmful but not necessarily illegal, such as disinformation or content that is harmful to minors.

Under the regulation, platforms that are accessible to minors (for instance if the T&Cs allow users under the age of 18) must take appropriate measures to ensure a "high level of protection of safety, security and privacy of minors"[34]. Rules are not further detailed. The recitals explain that this could be ensured for instance by "adjusting the default settings of the service interface"[35] since "the design of the interface could intentionally or unintentionally exploit the weaknesses and inexperience of minors."[36]

"Actual or foreseeable negative effects on the protection of minors" are also included within the list of systemic risks that VLOPs and VLOSEs must assess. Examples of mitigation measures (against the risk of exposure of minors to harmful content) include age verification and parental control.

Another important category of systemic risks addressed by the regulation is the dissemination of disinformation. Article 34 mentions "negative effects on civic discourse and electoral processes, and public security" or "on the protection of public health." Examples of mitigation measures include the "prominent marking" and a flagging system for deep fakes, discontinuing advertising revenue for specific information (or improving the visibility of authoritative information), and participating in codes of conducts.

It is interesting to see that if the EU faces a serious crisis (e.g. a pandemic or a war), endangering public health or security, the European Commission is empowered to require one or more VLOP or VLOSE to conduct a specific risk assessment and take specific mitigation measures.[37] Fundamental rights associations[38] criticise the excessive interference of the Commission, which can not only engage in a dialogue with providers to identify specific mitigation measures but also review them if the reported results are considered insufficient. The regulation establishes that these measures can be taken for maximum three months. However, this period can be extended. In addition, the Commission must encourage platforms to participate in the application of crisis protocols and for instance prominently display information on the crisis that is provided by the EU or member states. Also outside of a crisis, the Commission can invite relevant providers to participate in EU codes of conducts.

In the case of disinformation, the powers of the European Commission to direct how platforms address content during a crisis is considered particularly problematic because of the potential consequences on freedom of expression and citizen's rights to be informed.[39]

Also, content moderation polices regarding disinformation that are implemented by platforms are often contested. One emblematic case is the ban from YouTube (overturned afterwards) of a national UK radio, TalkRadio, for COVID-19 content that explicitly contradict expert consensus.[40]

06
SAFEGUARDS AGAINST ARBITRARY CONTENT MODERATION AND THE CASE OF MEDIA SERVICES

To protect users against arbitrary or erroneous moderation of their content, the regulation requires all platforms (including technical hosting service providers) to adequately in-

34 Article 28 of the DSA.

35 Recital 71 of the DSA.

36 Recital 81 of the DSA.

37 Arts.37 and 48 of the DSA.

38 Centre for Democracy and Technology "A series on the EU Digital services Act"

39 Will the Digital Services Act save Europe from disinformation? Centre for European Reform

40 BBC TalkRadio: YouTube reverses decision to ban channel.

form users in a timely manner every time they act against their content.[41] Also, online platforms need to give users the possibility to complain through an internal complaint-handling system that must have certain characteristics.[42]

Interestingly, platforms must do so not only when they remove content or suspend users accounts but also when they restrict at any degree the availability, visibility or monetization of content (e.g. when the ranking of content is decreased).

Further, online platforms must fairly process with a qualified staff (and not only by automated means) all the complaints they receive through the internal complaint-handling system and, where relevant, they must swiftly reinstate the disputed content or provide information about other redress possibilities.

Users are always entitled to refer the matter to courts but the regulation also allows them to seek a faster resolution (maximum 6 months) by referring the dispute to independent alternative dispute resolution entities that will need to be certified as such by the DSCs. These bodies do not have the power to impose binding decision to settle the dispute but the regulation obliges online platforms to engage in good faith with them.[43]

The regulation requires all intermediaries to inform users (in their T&Cs) of any restriction to the use of the service and to apply T&Cs fairly.[44] As far as restrictions are listed in T&Cs, it would seem that these providers remain free to restrict the use of the service beyond content that is illegal or harmful as defined in the DSA.

Users of platforms and search engines include media services and, as pointed out by the EU media associations, citizens increasingly access editorial media content (press, audiovisual, radio) online through the services of these providers.[45] The restriction of lawful content by media services on a social media, as well as the delisting of a whole media service from an app store or its down-ranking on a search engine, for its incompatibility with the service T&Cs, can have a great impact on citizen's freedom to receive information.

To protect media services (that are under the editorial responsibility of a regulated provider) from the interference of platforms, some members of the European Parliament had proposed the introduction of a media exemption,[46] which was however rejected.

Instead, with the same purpose but in a weaker way, the regulation requires platforms to consider freedom and pluralism of the media when applying their T&Cs.[47] Further, the regulation requires VLOPs and VLOSEs to include in their risk assessment the impact of the service on the exercise of fundamental rights, including "freedom of expression and of information" and "media freedom and pluralism," and take the appropriate mitigation measures.

Interestingly, following the adoption of the DSA, the European Commission decided to include some additional obligations for VLOPs regarding the moderation of regulated media services in a separate (sector-specific) legislative instrument that would apply on top of the regulation. The proposal for an EU Media Freedom Act ("EMFA") was adopted on 16 September 2022[48] and was at the time of writing, under scrutiny by co-legislators.

"The regulation requires all intermediaries to inform users (in their T&Cs) of any restriction to the use of the service and to apply T&Cs fairly

41 Art.17 of the DSA

42 Art. 20 of the DSA.

43 Art.21 of the DSA.

44 Art.14 of the DSA.

45 Joint statement by EU media association on the DSA trilogue.

46 On 14 Dec. 2021 the lead Consumer Protection and Internal Market (IMCO) Committee of the European Parliament rejected both Amendment 79 (new art.7a) of Opinion of Culture and Education committee and Amendment 281 (art.27anew) of Opinion of the Legal Affairs committee which were introducing the prohibition to interfere with, remove and suspend accounts of editorial content services that are published in compliance with the law.

47 "Diligent, objective and proportionate" (art.14).

48 Proposal for a regulation establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU.

The proposed obligations would apply to VLOPS as defined in the DSA but not to VLOSES and only in favour of media outlets that have self-declared to the platform (which is bound to provide the related functionality) that they are regulated in the EU as media services (including by widely recognised self or co-regulatory standards), and that they are independent from member states and third countries. It would seem therefore that it would be up to VLOPs (with the help of Commission's guidelines) to determine whether a media outlet fits with the criteria and that media outlets without an establishment in the EU would not be able to benefit from this media exemption.

In particular, VLOPS would be required to process complaints received by these media services (against any moderation of their content, on any ground) through a fast-track procedure.[49] Also, when they restrict content ("suspend the provision of the service in relation to that content") on T&Cs grounds, they would have to "take all possible measures" to provide a statement of reasons before their action takes effect (rather than in a timely manner), unless the content contributes to one of the systemic risks identified by the DSA (e.g. disinformation).

It is interesting to note that these obligations would not cover journalistic content that is provided outside of the editorial responsibility of a media (e.g. from citizen journalists). Also, contrary to similar provisions under discussion in the UK,[50] the proposal does not oblige the platform to refrain from taking action against the content while it reviews a complaint.

Finally, VLOPS would have to effectively engage in good faith in a dialogue "to find an amicable solution" with any of these media that requests it and that consider that the provider frequently restricts or suspends its content without sufficient grounds. They would also need to publish annual information on restrictions or suspensions of (regulated) media services on incompatibility grounds with the service's T&Cs. Information must include the number of instances and the grounds.

The European association of press publishers has criticised the proposal because it subjects the press to the interference of "not only platforms but also media regulators" to the detriment of press freedom.

According to the association, these "weak procedural safeguards do not remedy but rather further enshrines the right given by the DSA to large online platforms to censor legal editorial content on the basis of their terms and conditions."[51]

07
OTHER AREAS

The wide scope of the DSA is yet again apparent as it also deals with other aspects: online advertising,[52] recommender systems[53] and dark patterns.[54] In our view, these aspects do not fit comfortably in the DSA. While these are important provisions, it would have probably been best to address these areas in more horizontal pieces of legislation since there is no reason why they should be limited to intermediaries.

In a nutshell, the DSA aims to ensure that users are not forced into making a decision (e.g. giving their consent), can identify in real time each advert as such (including who paid for it) and are informed of the parameters used to target advertising to them and on how to change them. Users cannot be targeted with advertising on the basis of sensitive personal data (e.g. political opinion or sex orientation) or if they are minors. Users of VLOPs and VLOSEs must have access to an advertising repository. Platforms must also inform users in T&Cs on how their recommend content to users, and of options to modify the underlying parameters.

VLOPs must also provide one recommender system that is not based on profiling.

Indeed; all online websites, including editorial curated services, should avoid dark patterns and be subject to rules to protect users against online advertising and recommender systems.

49 Art.17 of the proposed EMFA.

50 UK government amendments on journalistic exception Online Safety Bill (section 16 Duties to Protect Journalistic Content).

51 ENPA statement of Sep. 2022.

52 Articles 26 and 39 of the DSA.

53 Articles 27 and 38 of the DSA.

54 Article 25 of the DSA.

A. Oversight and Enforcement

The DSA places a very large emphasis on the oversight and enforcement of the rules it introduces. [55] For all platforms, except for the obligations that only apply to VLOPS and VLOSEs, the member state where the intermediary is mainly established has the exclusive power of supervision and enforcement of the DSA, through national competent authorities. One of these authorities will need to be designated as a DSC by February 17, 2024.
This is a stark contrast, compared to the previous situation, where most of the services were not under the scrutiny of a sector specific national regulator. Some services (electronic communications services and video-sharing platforms in particular) are however already under the oversight of a sector specific regulator.

DSCs will be responsible for all matters relating to enforcement and supervision unless a member state decides to assign certain specific tasks or sectors to other competent authorities.[56] In all cases the respective tasks and competences of all authorities and the DSCs will need to be clearly defined and the names and tasks communicated to the European Commission and the to the newly created European Board for Digital Services.[57] At the time of writing, the member states were in the process of working out their institutional arrangements with various solutions envisaged, ranging from awarding the DSC status to the media regulatory authority, the competition authority, the electronic communications authority or to a newly created authority (other solutions are also envisaged). These institutional arrangements are far from simple because as explained above, the DSA covers many types of intermediaries and because many areas are covered, which means that multiple authorities may be well placed to supervise the application of the rules.

B. VLOPS and VLOSES to be overseen by the European Commission

After a lot of discussions, the European Commission was given the exclusive power to oversee the additional obligations that are incumbent on the VLOPS and VLOSES (or if they have systematically infringed the other provisions of the regulation).[58] To cover the costs of supervision, the DSA foresees that these operators will need to pay an annual supervision fee to the Commission, which will be determined by the Commission through the adoption of a delegated act, and which will take into account the costs incurred in the previous year while being proportionate to the number of monthly recipients of the platforms. In any case, the fee will not be able to exceed 0.05 percent of the platform's worldwide annual net turnover of the preceding year. Nothing is foreseen on the supervision fees that may (or not) be levied at the national level, whereas the DSA foresees that the authorities in charge should be independent and sufficiently funded.[59]

> ***DSCs will be responsible for all matters relating to enforcement and supervision unless a member state decides to assign certain specific tasks or sectors to other competent authorities***

Also, to facilitate the oversight of the large platforms, other measures are introduced. First, just like in the financial sector, independent auditors will need to assess whether they comply with their due diligence obligations as well as the commitments they make through code of conduct and crisis protocols. In case of a negative audit report, the VOPS and VLOSES will need to publish an audit implementation report explaining how they intend to remedy the situation.[60] Second, like in the GDPR,[61] a compliance function is foreseen whereby compliance officer(s) are responsible for cooperation with the DSCs and the European Commission and who will be responsible for informing and advising the management and staff about the obligations of the DSA. Then, very interesting mechanisms are foreseen on giving access to vetted researchers (and to the DSCs and the European Commission) to data held by VLOPS and VLOSEs to help them conduct research on systemic risks

55 Chapter 4 of the DSA.

56 Article 49 of the DSA.

57 Article 61 of the DSA.

58 Article 65 of the DSA.

59 Article 43 of the DSA.

60 Article 37 of the DSA.

61 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

and risk mitigation measures.[62] Among the many investigation powers that are given to DSCs and the Commission, we also flag the fact that VLOPS and VLOSEs can be ordered by the Commission to provide them access to their algorithms.[63]

VLOPS and VLOSEs could be fined up to 6 percent of their total annual word turnover if they are found to be in breach of the regulation.[64]

08 CONCLUSIONS

In short, on paper the DSA is certainly what it set out to be: a horizontal EU wide regulation covering intermediary services by establishing specific due diligence obligations tailored to specific categories of providers of services.

In practice however, it may be difficult to put into application.

First because it covers a very wide range of service providers, including the technical internet intermediaries. More fundamentally the scope of the illegal harms seems particularly wide. All types of illegal content are treated in the same way except for certain caveats, which could mean that platforms could be flooded with requests to take down content. There are no mechanisms to help the platform to determine if the national law that could be breached is in line with EU legislation, which may also cause problems for them.

Platforms are obliged to include in their T&Cs their content moderation policies and to supplement some of the rules of the DSA, and in particular those on the suspension of users and on the risk mitigation measures to be taken. However, it is our understanding that platforms remain free to restrict the use of the service beyond content that is illegal or harmful as defined in the DSA.

Therefore, although it is laudable that users are informed of and entitled to complain against all moderation decisions (including down-ranking or demotions), platforms may once more be flooded with requests, in particular because complaints must be subject to human review. In practice, and if online platforms encounter such difficulties, the rights of users will ultimately be undermined. It is true however that users can always refer the matter to alternative dispute resolution bodies but platforms (and users) could potentially refuse to accept their decisions, since the DSA foresees that their decisions are not binding.

Regretfully the DSA did not specifically address the issue of the moderation of media outlets by the larger platforms and even before the DSA was adopted, the Commission had already proposed rules to protect the integrity of media services on VLOPs in another legal instrument, the EMFA.

> ***"Regretfully the DSA did not specifically address the issue of the moderation of media outlets by the larger platforms and even before the DSA was adopted***

The obligation to conduct a risk assessment (and eventually take mitigation measures) on the impact of the service on freedom of expression, and freedom and pluralism of the media, is extremely wide and could also be difficult to deliver in practice.

This broad scope of application is also reflected in added areas that are addressed in the DSA, namely the rules on dark patterns, recommender systems and online advertising, which in our view do not comfortably sit in the DSA.

The European Commission has a fundamental role to play in the follow-up to the DSA. First it will be the sole enforcer of the added rules that apply to VLOPS and VLOSES, although many new mechanisms are foreseen such as independent auditors, the compliance function and the possibility for vetted researchers to get access to data belonging to VLOPS and VLOSEs. Also, it will be allowed in case of crisis to directly interfere with the choice of measures including to address disinformation.

Lastly, the Commission has the power to adopt guidelines, delegated and implementing acts, and to promote voluntary standards. In some areas, it will be particularly interesting to see to what extent the Commission will use these powers, which no doubt will help to shed more light on some of the concepts of the DSA.

62 Article 40 of the DSA.

63 Article 72 of the DSA.

64 Article 74 of the DSA.

In terms of enforcement, more generally, the DSA marks a shift in approach and places a lot of responsibility on national DSCs, which will need to be designated by 17 February 2024.

It remains to be seen however if these national authorities and the European Commission will be sufficiently well funded and equipped to carry out in a proper way their supervision and enforcement tasks under the DSA.

> *The European Commission has a fundamental role to play in the follow-up to the DSA*

YOU MAY BE SUBJECT AS WELL!: DIGITAL SERVICES ACT – WHAT COMPANIES NEED TO KNOW

BY JULIA APOSTLE

& KELLY HAGEDORN

& CHRISTIAN SCHRODER

& ADELE HARRISON

Julia Apostle, Partner at Orrick Paris; Kelly Hagedorn, Partner at Orrick London; Christian Schröder, Partner at Orrick Germany & Adele Harrison, Managing Associate at Orrick London.

01 WHY SHOULD COMPANIES BE READING THIS?

Even though the new EU's Digital Services Act ("DSA") [2] will impose many new compliance and reporting requirements for many businesses, most businesses have not yet started preparing as they may consider the DSA to only apply to the Big Tech companies. This is a misunderstanding. The DSA applies to many more companies than just Big Tech. By Febru-

2 Formal title: Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

ary 2023, companies will need to demonstrate compliance with initial notification requirements.

This article provides a brief overview on "who should comply" with the DSA and we will summarize the main requirements.

02

WHO MUST COMPLY WITH THE DSA? JURISDICTION AND KEY DEFINITIONS

The DSA applies to “intermediary services offered to “recipients of the service” that have their place of establishment or are located in the EU. The location of establishment of the intermediary service outside of the EU will not prevent application of the law.

An “intermediary service” basically covers all companies which show/process third party content on their website. Even a mere "comment function" on a website allowing third parties to share their views may trigger the application of the DSA.

More specifically, the DSA defines "intermediary service" as a “mere conduit” service, “caching” services, “hosting” services and “online search engines.” Hosting services are further divided into “online platforms” and “very large online platforms” (“VLOPs”). There is also a sub-category of “very large online search engine” (“VLOSE”).

A “recipient of the service” is defined as a “natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible.”

The nature and scope of the obligations applicable to an intermediary service depend on the classification of the intermediary service provider into one of these categories. Therefore it will be important to assess whether an online service provider qualifies as an intermediary and, if so, which category of intermediary. At one end of the spectrum, with most obligations, are VLOPs and VLOSEs. At the other end, with the least number of requirements with which to comply, are “mere conduits” and “caching” services. The categories are defined by the DSA as follows:

- A “**mere conduit**” transmits information provided by a recipient of the service in a communication network, or provides the access to a communication network (examples include VPNs, wireless access point, internet exchange points, top-level domain name registries).
- A “**caching**” service involves the automatic, intermediate, and temporary storage of information transmitted in a communication network of information provided by a recipient of the service (examples include database caching, web caching).
- A “**host**” stores information provided by and at the request of a recipient of the service (examples include cloud storage services, online platforms).
- An “**online platform**” is a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public (examples include online marketplaces, social networks, collaborative economy platforms). If the storage and dissemination functionality is only a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, then it will not be considered as an online platform but may still qualify as a host.
- An “**online search engine**” is a digital service that allows users to input queries in order to perform searches of a website or all websites, in a particular language in the form of a keyword, voice request, phrase or other input, and return results in any format (examples include Google search, Bing, Brave, and others).

The decision to designate an online platform as a VLOP or VLOSE is made by the European Commission, provided the platform has a number of average monthly recipients of the service that is higher than 45 million. The definition of an “active recipient of an online service” is not necessarily the same as an “monthly active user,” which is a common measure of site engagement. Under the DSA, an active recipient is a “recipient of the service that has engaged with an online platform, either by requesting the online platform to host information or being exposed to information hosted by the online platform and disseminated through its online interface.”

03

WHEN DOES THE DSA TAKE EFFECT ?

The obligations of the DSA come into effect in a staggered manner. The very first obligation must be complied with by **February 17, 2023,** which is just around the corner. Article 24(3) of the regulation requires online platforms and online

search engines to publish, on their website, starting February 17, 2023 and at least every 6 months thereafter, the number of average active monthly recipients of the service.

Most of the other obligations come into force by February 17, 2024, except that the VLOPs and the VLOSEs are subject to a much shorter compliance timeframe.

04
NATURE OF THE OBLIGATIONS

As already noted, the application of obligations depends on the nature of intermediary service, and even the minimal requirements may be considerable for individuals businesses.

All intermediary service providers will be required to do the following:

i. Act against items of illegal content (e.g. take them down) and/or provide the requested information about individual service recipients upon receipt of a duly issued order by the relevant national authority (the DSA specifies the conditions to be satisfied by such orders). The concept of "illegal content" is defined as "information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law." Thus, the application and interpretation will vary from Member State to Member State and may thus require significant resources on the company's side when determining what content is illegal and in which jurisdiction.
ii. Identify a single point of contact within the organization who will be the point of contact for liaison with national authorities. Intermediaries that do not have an establishment in the EU will have to appoint a legal representative in a Member State where the intermediary offers its services (there may be a possibility of collective representation for micro, small, and medium enterprises). Since, however, the representative will be liable for actions of the represented company, it may not be easy to find such representatives.
iii. Comply with specific obligations in relation to the form and content of the intermediary service terms and conditions. For instance, the terms must be fair, non-discriminatory, and transparent, and must include information regarding how to terminate services, restrictions imposed on the delivery of services, and also regarding the use of algorithmic tools for content-moderation. Details of rules of internal complaints handling systems should also be disclosed.
iv. For services provided to minors or pre-dominantly used by them, the terms must be expressed in easily understandable language.
v. Protect the anonymity of users except in relation to traders.
vi. Publish an annual transparency report on any content moderation then engaged in, including specified information such as the number of orders received from Member States' authorities, response times, and information about the own-initiative content moderation practices of the service, including the use of automated tools and the restrictions applied, and information about the training and assistance provided to moderators. (This obligation does not apply to micro or small enterprises that do not qualify as very large online platforms). These obligations, and others, will require the implementation of specific internal processes in order to capture the required information.

"The application of obligations depends on the nature of intermediary service, and even the minimal requirements may be considerable for individuals businesses

Additional obligations for hosting services, including online platforms include the following:

i. Hosting services must have a notification mechanism allowing the signalling of content considered by a user to be illegal content. The mechanism must be designed to facilitate sufficiently precise and substantiated notices to permit the identification of the reported content.
ii. Hosting services must provide a statement of reasons to the user if their content is disabled or removed or if services are suspended. This explanation must contain certain information, including the facts relied upon and a reference to the legal ground relied upon, or other basis for the decision if it was based on the host's terms and conditions. However, law enforcement authorities may request that no explanation is provided to users.
iii. There is a positive obligation to alert law enforcement or judicial authorities if the host suspects that a serious criminal offence involving a threat to life or safety of persons is taking place or is planned.

iv. The anonymity of the content reporter is to be protected, except in relation to reports involving alleged violation of image rights and intellectual property rights.
v. The transparency reports prepared by hosting services will have additional information, including the number of reports submitted by trusted flaggers and should be organized by type of illegal content concerned, specifying the action taken, the number processed by automated means and the median response time.

The additional obligations for online platforms include the following. The obligations in this section do not apply to micro or small enterprises, except if they qualify as very large online platforms. Intermediary services may apply to be exempted from the requirements of this section of the DSA.

i. Online platforms must provide an appeal process against decisions taken by the platform in relation to content that is judged to be illegal or in breach of the platform's terms and conditions. The relevant user will have six months to appeal the decision. Decisions must not be fully automated and must be taken by qualified staff.
ii. Users will be able to refer decisions to an out-of-court dispute settlement body certified by the Digital Services Coordinator of the relevant Member State. Clear information regarding this right must be provided on the service's interface.
iii. Content reported by trusted flaggers must be processed with priority and without delay. An entity may apply to the Digital Services Coordinator to be designated as a trusted flagger, based on criteria set out in the DSA.
iv. The suspension of users, for a reasonable period of time, is permitted if they repeatedly upload illegal content, after issuing a prior warning. Online platforms must also suspend the processing of notices and complaints from users that repeatedly submit unfounded notices and complaints.
v. Online platforms are required to ensure that their services meet the accessibility requirements set out in the EU Directive 2019/882, including accessibility for persons with disabilities, and must explain how the services meet these requirements.
vi. There is a specific prohibition applicable to online platforms in relation to the use of "dark patterns." The European Commission may issue further guidance in relation to specific design practices. The prohibition does not apply to practices covered by the Directive concerning unfair business-to-consumer practices, or by the GDPR.
vii. To ensure the traceability of traders (i.e. professionals that use online platforms to conduct their business activities), online marketplaces must only allow traders to use their platform if the trader first provides certain mandatory information to the platform, including contact details, an identification document, bank account details, and details regarding the products that will be offered. Online platforms must make best efforts to obtain such information from traders that are already using the platform services within 12 months of the date of coming into force of the DSA.
viii. A trader who has been suspended by an online platform may appeal the decision using the online platform's complaint handling mechanism.
ix. Online platforms that allow consumers to conclude distance contracts with traders through their services must design their interface so as to enable traders to provide consumers with the required pre-contractual information, compliance and product safety information. Traders should be able to provide clear and unambiguous identification of their products and services, any sign identifying the trader (e.g. a logo or trademark), and information concerning mandatory labelling requirements.
x. Online platforms must make reasonable efforts randomly to check whether the goods and services offered through their service have been identified as being illegal. If an online platform becomes aware that an illegal product or service has been offered to consumers it must, where it has relevant contact details or otherwise by online notice, inform consumers of the illegality and the identity of the trader, and available remedies.
xi. To promote online advertising transparency, online platforms must ensure that service users receive the following information regarding online ads: that the content presented to users is an advertisement, the identity of the advertiser or person that has financed the advertisement, information regarding the parameters used to display the ad to the user (and information about how a user can change those parameters).
xii. Targeting techniques that involve the personal data of minors or sensitive personal data (as defined under the GDPR) is prohibited.
xiii. Online platform providers must provide users with functionality that allows them to declare that their content is a "commercial communication" (i.e. an advertisement / sponsored content).
xiv. Online platforms have transparency obligations regarding any recommender system that is used to promote content. The online platform must disclose the main parameters used, as well as options for the recipient to modify or influence the parameters.

"The obligations in this section do not apply to micro or small enterprises, except if they qualify as very large online platforms

Additional obligations for VLOPs and VLOSEs include the following:

i. VLOPs and VLOSEs must publish their terms and conditions in the official languages of all Member States where their services are offered (this is often a requirement of national consumer protection law as well).
ii. VLOPs and VLOSEs must carry out (and in any event before launching a new service), an annual risk assessment of their services. The risk assessment must take into account in particular risks of dissemination of illegal content; negative effects for the exercise of the fundamental rights; actual or foreseeable negative effects on civic discourse and electoral processes and public security; in relation to gender-based violence; public health; minors; and physical and mental well-being. VLOPs and VLOSEs must consult with user representatives, independent experts and civil society organizations.
iii. VLOPs and VLOSEs must implement mitigation measures to deal with these systematic risks. The DSA lists measures that might be adopted.
iv. VLOPs and VLOSEs must have independent audits carried out at least once a year, by independent firms, to assess their compliance with the DSA requirements and any commitments undertaken pursuant to a code of conduct. The DSA imposes certain conditions on the firms that must conduct such audits (e.g. they must be independent and free of conflicts of interest).
v. VLOPs and VLOSEs may be required by the Commission to take certain specified actions in case of a crisis, including conducting an assessment to determine whether the service is contributing to the serious threat and to adopt measures to limit, prevent or eliminate such contribution.
vi. VLOPs that use recommender systems must provide at least one that is not based on profiling and must provide users with functionality to allow them to set their preferred options for content ranking.
vii. Additional advertising transparency obligations are applicable, requiring the publication of information regarding the advertisements that have been displayed on the platform, including whether the advertisement was targeted to a group, the relevant parameters and the total number of recipients reached. The information should be available through a searchable tool that allows multicriteria queries.
viii. VLOPs and VLOSEs are required to share data with authorities, where necessary for them to monitor and assess compliance with the DSA. Such information might include explanations of the functioning of the VLOPs algorithms. The regulator may also require that VLOPs allow "vetted researchers" (those that satisfy the DSA's requirements) to access data, for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks.
ix. VLOPs and VLOSEs must appoint a compliance officer responsible for monitoring their compliance with the DSA.
x. VLOPs and VLOSEs must pay the Commission an annual supervisory fee to cover the estimated costs of the Commission (the amount is still to be determined).

05
OTHER KEY ELEMENTS OF THE DSA

A. Intermediary Liability

The DSA retains the exemption contained in the eCommerce Directive, which provides that intermediaries are not liable for information transmitted through their services, provided they were not actively involved in the transmission and/or they acted to remove or disable access to the information upon receiving notice. There is a modification to this exemption with the DSA, in that it imposes on hosts (and the subset categories of online platforms and very large online platforms) a set of due diligence requirements in relation to illegal content, as described above in relation to specific obligations. In addition, the text retains the principle that intermediaries will not be subject to a general monitoring obligation, however as stated in Recital 30, "this does not concern monitoring obligations in a specific case."

B. Interaction With Other Laws

Importantly, the DSA does not override existing EU and national legislation and therefore there will be areas of overlap among the DSA obligations and those set out in other laws. For instance, both the DSA and the EU Platform to Business Regulation 2019/1150 contain transparency and operational requirements in relation to the use of recommender systems. The Online Terrorist Content Regulation 2021/784 also contains specific notice and action obligations in relation to terrorist content, and both the Audiovisual Media Services Directive 2010/13/EU and the EU Copyright Directive 2019/790, as implemented nationally, cover some of the same ground. Since compliance with some of the DSA requirements will be facilitated by the use of AI technology, the EU's AI Act, which is currently close to adoption, will also need to be taken into consideration. And of course, the various EU Member States have their own laws applicable to illegal content – not to mention differing standards as to what constitutes illegal content.

In practical terms, this means that companies subject to the DSA should not only be identifying the obligations in that law with which they must comply, but also how their DSA obligations intersect with other applicable legal requirements. Companies should also take note of the different national enforcement authorities that may have competence in relation to the overlapping legal obligations. In France, for instance, it is the consumer rights authority ("DGCCRF") that is responsible for enforcing the Platform to Business Regulation, but it will likely be Arcom that is the Digital Services Coordinator (see the section on Enforcement, below). National data protection authorities will also have a role, given that certain of the DSA provisions deal with the processing of personal data (see below).

C. Impact for the Online Advertising Ecosystem

The transparency obligations imposed on online platforms in relation to the advertising on their sites will most certainly result in the contractual flow-through of DSA obligations to participants in the online advertising ecosystem that are not directly subject to the regulation. For example, the obligation to ensure that online ads are appropriately identified as such, and that users are informed of the identity of the advertiser and of applicable targeting parameters, may require cooperation of ad tech providers. In addition, the prohibition against ad targeting based profiling, as defined by the GDPR, using sensitive personal data, will also pose technical compliance problems, especially in light of European Court of Justice's recent case law that adopts a very broad approach to the definition of special category data, specifically including indirectly inferred information.[3]

06
SANCTIONS & ENFORCEMENT

A. Sanctions

Temporary access restrictions. Where enforcement measures are exhausted, and in the case of persistent and serious harm, the Digital Services Coordinator may request that the competent judicial authority of the Member State order the temporary restriction of access to the infringing service or to the relevant online interface.

Fines. Sanctions must be "effective, proportionate and dissuasive." Member States must ensure that the maximum number of penalties imposed for a failure to comply with the provisions of the DSA must be 6 percent of the annual worldwide turnover of the intermediary or other person concerned. The maximum amount of a periodic penalty payment must not exceed 5 percent of the average daily turnover of the provider in the preceding financial year per day.

B. Enforcement

Each Member State must designate one or more competent authorities as responsible for the application and enforcement of the DSA, and one of these authorities must be appointed by the Member State as its Digital Services Coordinator. Except for the VLOPs and the VLOSEs, this Digital Services Coordinator will be the main enforcement authority. For non-EU based intermediaries, the competent Digital Services Coordinator will be located in the Member State where these intermediaries have appointed their legal representative. If no legal representative has been designated, then all Digital Services Coordinators will be competent to act. The European Commission will have exclusive jurisdiction in relation to enforcement of the obligations specifically applicable to the VLOPs and VLOSEs, and may assume jurisdiction to enforce other obligations against the VLOPs and the VLOSEs.

Digital Services Coordinators are granted investigation and enforcement powers — including the power to accept intermediary services' commitments to comply with the DSA, order cessation of infringements, impose remedies, fines, and periodic penalty payments.

A recipient of the service has the right to lodge a complaint against providers of intermediary services alleging an infringement of the DSA with the Digital Services Coordinator of the Member State where the recipient resides or is established.

3 See https://curia.europa.eu/juris/document/document.jsf;jsessionid=5CBD746EB4FD0D8B4D0DC7461B5B0129?text=&docid=263721&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8887343.

07
WHERE TO START

Companies with an online presence should already be determining whether they are subject to the terms of the DSA by virtue of qualifying as an online intermediary. If so, does the company offer its services in Europe and does it have an establishment in Europe? It may be necessary to identify and appoint a potential legal representative.

In parallel, following classification into a category of intermediary, it will be necessary to identify the applicable obligations, and the different teams or individuals within the company who will be part of implementing a compliance strategy. Cross-functional collaboration from the outset will be essential.

And do not forget the reporting obligation from February 2023.

Companies with an online presence should already be determining whether they are subject to the terms of the DSA by virtue of qualifying as an online intermediary

CONTENT MODERATION AND COMPETITION IN DIGITAL MARKETS

BY MACIEJ SOBOLEWSKI

& NÉSTOR DUCH-BROWN

Joint Research Centre - European Commission. The opinions expressed in this article are the authors' and do not necessarily reflect those of the European Commission.

01 INTRODUCTION

The past 20 years or so have witnessed the rapid development of novel digital services, based on the notion of the social web or Internet 2.0. This innovation in the way digital content was generated and consumed has provided abundant value to consumers and at the same time has allowed the emergence of new firms and business models that have completely changed the competitive landscape of digital markets. However, the legal and regulatory framework in which these developments

took Place was designed still having in mind the characteristics of the previous phase of the development of the internet. In that period, content was mostly consumed in a passive manner from static websites offered by a relatively small number of content producers. Although there was misinformation and illegal activities also at that time, technology was a rather small industry, and it did not affect most people's lives in a significant way. Today, when software and algorithms have become mainstream, all the problems we face as a society have a manifestation based in software and algorithms as well. As a greater proportion of individuals adopt digital solutions and start using them regularly, the online world replicates the good and bad things that happen in the offline world. However, in the online dimension the problems are amplified not only because they involve a lot more people, but because they combine and feed each other and generate new externalities. In a novel online setting with emerging new actors in economic and social activities, there is a need to rethink the rules of the game.

In what follows, we focus on these new rules included in the Digital Services Act ("DSA"). However, instead of taking a fundamental rights approach, we will look at it from a competition perspective. Since the DSA has been less frequently approached from this perspective compared to the Digital Markets Act ("DMA") – aiming at increasing contestability of digital markets-, we think we offer a somewhat novel perspective. We argue that the DSA, via the modification of liability rules for platforms, may also bring competitive effects to the platform economy. We structure our thinking as follows. First, we discuss why an update of liability regime was necessary in the first place. Second, we sketch some mechanisms that explain how platforms may adapt to the new rules and we argue that more content screening can be expected. Third, we hypothesize how the DSA may affect competition between large and small platforms via changes in content curation behavior. We delineate some scenarios under which the existing differences in size between the platforms could decrease leading to a more balanced market landscape.

02
WHY DO WE NEED THE DIGITAL SERVICES ACT?

The current legal framework for online activities was set out in the Electronic Commerce Directive ("ECD") more than twenty years ago when the Internet ecosystem was in still in a nascent phase. Over these two decades, the types of online services have evolved substantially, and so has the scale of their use. The role of providers changed from the provision of mere conduit to the creation of services based on data while leveraging positive externalities among users. Finally, a new type of private enterprises acting as online intermediaries on multisided markets emerged on the digital scene.

These platforms orchestrate interactions among various types of participating users. Because of their huge success in facilitating online transactions and exchanges of user generated content of all sorts, these online platforms quickly expanded to complex and powerful ecosystems. These ecosystems have now a systemic impact on the economy and society, occurring in both intended and unintended ways. For example, recent research extensively discusses the side-effects of the widespread use of recommender algorithms by social media on contagious spread of propaganda and fake news. On the other hand, the Facebook-Cambridge Analytica scandal demonstrated how user data can be abused for psychological targeting or worse, manipulation of political preferences according to a hidden private agenda. To address these systemic challenges and ensure better protection of users and their fundamental rights in the rapidly growing digital space, the European Commission decided that the legal framework for online activities needed a modernization. The DSA introduces updated harmonized liability rules for all providers of digital services on the Digital Single Market. Additional measures are also imposed on very large online platforms (reaching more than 45 million users in the European Economic Area) of various types: search engines, marketplaces and social networks, in recognition of their pivotal role for the mitigation of systemic risks, such as manipulation of elections, censorship, spread of disinformation, illegal hate speech, cyber violence or harm to minors.

The ECD liability regime was established in 2000, when major digital services like social media and big online marketplaces were yet non-existent. Without an exemption from primary liability for service providers, the online services as we know them today would not have developed because of litigation costs. In the ECD, conditions for liability exemption are linked to the so-called knowledge-standard. They apply mostly to providers who host content uploaded by third parties. A platform hosting particular item like pirated movie, or a racist post will not be held liable as long as it is not aware of its illegal nature. Once the platform learns about a concrete infringing item, it has to block it in order to maintain liability exemption. This action has to be expeditious and preceded by an appropriate evaluation. A platform may enter into possession of a "red flag knowledge" in two ways. It may discover the infringing item via own screening procedure such as filtering or automated content moderation or by receiving a notification from a third party that located the item on particular account administered by the platform. While the above rules are logically consistent, it is not hard to see why they may not be fit for purpose when user-generated content is being uploaded at a scale of billions items every hour. There is a legitimate concern

that hosting services would choose to limit the inflow of the red flag knowledge from third parties rather than engage in costly handling of infringing items. This dysfunctional outcome could be easily accomplished with small modifications of user interface that deteriorate user-friendliness of reporting process. Against this opaque incentive that leads to less illegal content being blocked, the DSA pushes for greater empowerment of the third parties coupled with more active engagement in content management by the platforms, both leading ultimately to higher suppression of illegal items.

Importantly, the new regulation does not force the platforms to engage in moderation of all uploaded content items nor imposes any technical solutions with regard to content curation. Such obligation would quickly generate a prohibitive economic burden on smaller online providers who experience rapid growth in content volumes. Indeed, content moderation requires a great deal of financial resources, skills and labor. Automated moderation based on machine learning algorithms does not guarantee perfect accuracy in detecting truly infringing items. Despite the overall technical progress over the past years, misclassification rates are often high and there are no magical shortcuts. For example, an increasing proportion of true negatives always comes at the costs of rejecting more legitimate items, which leads to undesirable over-moderation. This shows that human judgement still is crucial in the process and will remain so in the near future. Human moderation can be from 5 to 20 times more expensive than AI-based moderation depending on the type of content and wages on the local labor markets. This makes the entire business process not scalable. Human moderators work usually only in "grey zone" cases, those that require advanced contextual judgement. Largest online platforms contract several thousands of moderators and their total wage bill for content moderation is counted in hundreds of millions of dollars annually.

To achieve its main goal of ensuring better protection to users and to fundamental rights online, the DSA introduces a seemingly minor modification to the conditions required for the safe harbor. Yet this change has far-reaching consequences for the behavior of the platforms. In order to maintain liability exemption all online platforms must implement a new, user-friendly notice and action procedure that simplifies the notification of specific items considered to be illegal by the notifying parties. In practical terms, this procedure facilitates submission of notices about potentially harmful elements by third parties, in particular private persons, copyright holders and rights enforcement organizations who have legitimate interest in screening content. If the platform agrees with the assessment of the notifying party, it has to swiftly remove or disable access to that content. Additionally, the platform is obliged to instate an efficient complaint and redress mechanism and to allow trusted flaggers who may place notifications on a mass scale. Similarly to the ECD, the DSA presumes that a platform acquires a "red flag knowledge" about a particular infringing element upon receiving a valid notice, which includes information on the internet location of that element. Easily accessible notifications guarantee that avoiding a "red flag knowledge" will be practically impossible.

Submitted notices are quite costly to handle, as typically they will require human evaluation and processing. This is why the DSA, while presuming diligence and good faith of all parties, contains also safeguards against placing unfounded notices on a mass scale that abuse the notice and action mechanism. If a platform decides to reject the notice, it has to provide a written justification which may be contested by the affected user, possibly escalating to out-of-the-court dispute settlement level. By increasing the ease of submitting notices, the DSA provides additional economic incentives for the platforms to engage, at least partially, in own *ex ante* content screening to reduce the number of legitimate notices to deal with. This outcome can be achieved with hash-based filtering, which compares newly uploaded content against already blacklisted items and also *ex ante* automated moderation approach. It is important to note that the business process leveraging the abovementioned technologies can either be developed in-house or outsourced to third-party providers offering content moderation in a software-as-a-service mode. The choice between both options is determined by platform scale. For sufficiently large content volumes, own custom-made solution will be more cost effective per item than the unit price of a third-party solution, although it requires substantial upfront investment.

03

HOW WILL PLATFORMS REACT TO THE DSA?

In the previous section we argued that the updated liability rules, and most notably the notice-and-action procedure, may push platforms towards more intensive content screening to avoid overflow of notices. Additional *ex ante* screening efforts and scrutinizing items flagged in the notices will result in higher curation of user-generated content and less counterfeited products available online. Better quality of content-based services will likely increase satisfaction of various user groups on a platform. However, users will also face a price to pay for the efforts undertaken by the platform operator.

As any profit maximizing entity, a platform will react to the increased volume of notices and additional screening effort by increasing the price for its services. In this way, a platform will try to shift the increased cost of content curation on one or more groups of users. This pass-through effect

may take different forms in practice, depending on the type of a platform and adopted business model. For example, a social network could widen the scope of data requested from users in exchange of the service or increase their exposure to ads. Instead of rising the implicit price denominated in data, a social network could also increase monetary fees for advertisers. Similarly, a marketplace operator might lift transaction fees for business users to recover part of the costs related to tracking counterfeited goods. Economic models of multi-sided markets suggest that in order to absorb a cost increase, a monopoly or a dominant platform will exploit in the first place the group of users with less elastic demand. Typically this will be advertisers or business users, who are less likely to quit due to limited substitutability of their target audiences. Monetization of data is often combined with service innovation to derive more value from economies of scope in data aggregation. For example, a platform that has widen scope of collected data may expand to adjacent markets in order to add complementary services to its core offering. Such ecosystem expansion strategy will reduce the negative effects of price adjustment on current users.

Intuitively, a pass-through effect on users will be determined by several factors, such as (i) adaptation costs for the platform related to additional content screening triggered by the DSA; (ii) users' taste for quality of content and (iii) privacy preservation; and (iv) proportion of captive users in the total user base of a platform. Contrary to contestable users, captive users are loyal and thus can be easily exploited by the platform. The pass-through will also depend on the degree of horizontal differentiation between competing platforms, which determines the competition effects on the contestable segment. It can be expected that, ceteris paribus, larger platforms will be able to pass a greater proportion of costs on users than smaller platforms. This is caused by the difference in network externalities that favors a larger platform. On the other hand, larger platforms may not necessarily bear a higher level of adaptation costs induced by the DSA due to the two opposing effects at play. The first effect is positive for big platforms and relates to economies of scale from in-house content moderation. Bigger platform have access to the better AI skills, larger training datasets and cheaper storage and computing power, which all provide for higher detection precision in comparison to software-as-a-service external solutions. Consequently larger platforms will enjoy lower per item cost of automated moderation. The second effect is negative and related to a greater content scrutiny by trusted flaggers. Intuitively, the attention of trusted flaggers, copyright owners and other monitoring organizations will naturally be focused on dominant platforms where harm from illegal content is amplified because of large network externalities. Consequently, a bigger platform will receive more notices to handle diligently in order to preserve liability exemption. It is impossible to say which of the two effects prevails a priori, especially because large and small platforms may differ in other relevant factors, such as audience profile, organic rate of content toxicity, moderation technology used to date, which also determine the level of adaptation costs to the DSA.

04
WHAT ARE POSSIBLE COMPETITION EFFECTS OF THE DSA?

Based on the previous considerations, we argue that the DSA will likely result in more intensive screening and curation of content on the platforms side, leading to higher costs of service provision. The magnitude of the cost increase will vary across platforms in a complex way. As discussed above, the per item adaptation costs may not necessarily be higher for big platforms, although most likely they will be able to shift a greater proportion of this cost to users. For these reasons, various outcomes with regards competition effects of the DSA may materialize.

In general terms, competition between platforms will be stronger, the larger the segment of contestable users and the less differentiated the service. However, bigger platforms also enjoy an incumbency advantage, stemming from direct and indirect network externalities. This "bigness" advantage translates into more loyal (captive) consumers on average, which cannot easily be captured by other platforms via higher content quality or lower price. The big platform will need to balance the opposing incentives to exploit its captive users while competing with other platforms for contestable consumers. Additional screening effort enables platforms to leave more utility to users from enjoying less toxic environment. On the contestable part of the market, this additional utility will attract new users. This indirect positive competition effect reduces a pressure on platforms to increase the price. On the other hand, a platform faces an increase of its marginal cost of serving users, which it will try to shift onto users via increased price (monetary or implicit). The aforementioned effects have opposite signs, but when additional screening costs are high, the pass-through effect is likely to outweigh competition effect. In such case, a platforms will react to the DSA by increasing prices more -ceteris paribus- than in the case of low adaptation costs. On the other hand, if the DSA adaptation cost is small, the competition effect will prevail, and the platform could lower its price to attract more customers.

Building on the above considerations, there are four qualitatively different outcomes of completion between large

and small platforms that may occur with the DSA: all platforms increase or decrease their prices; big (small) platforms increase the price while small (big) decrease it. A priori none of these options can be ruled out and in fact they may appear simultaneously on various multisided markets. For the two asymmetric options, the consequences for market equilibrium are clear. If only the big platforms adjust their prices upwards, the DSA will have a levelling effect on the market. A smaller platform will gain more users, and will in turn attract more advertisers. Under this scenario, the DSA will increase the financial viability of the smaller platforms and will diminish the size asymmetry. If however, big platforms decrease their price while the small ones increase it, the existing differences will be further amplified leading to an even more cornered market outcome. In the third scenario with low content curation costs for all platforms, competition could result in providing higher quality of content to users at unchanged or lower prices. Such an outcome would be preferable from a social welfare perspective. It could be supported by a number of policy measures aiming at reducing the costs of moderation for all small platforms by improving access to cloud infrastructure, large training data sets and AI skills.

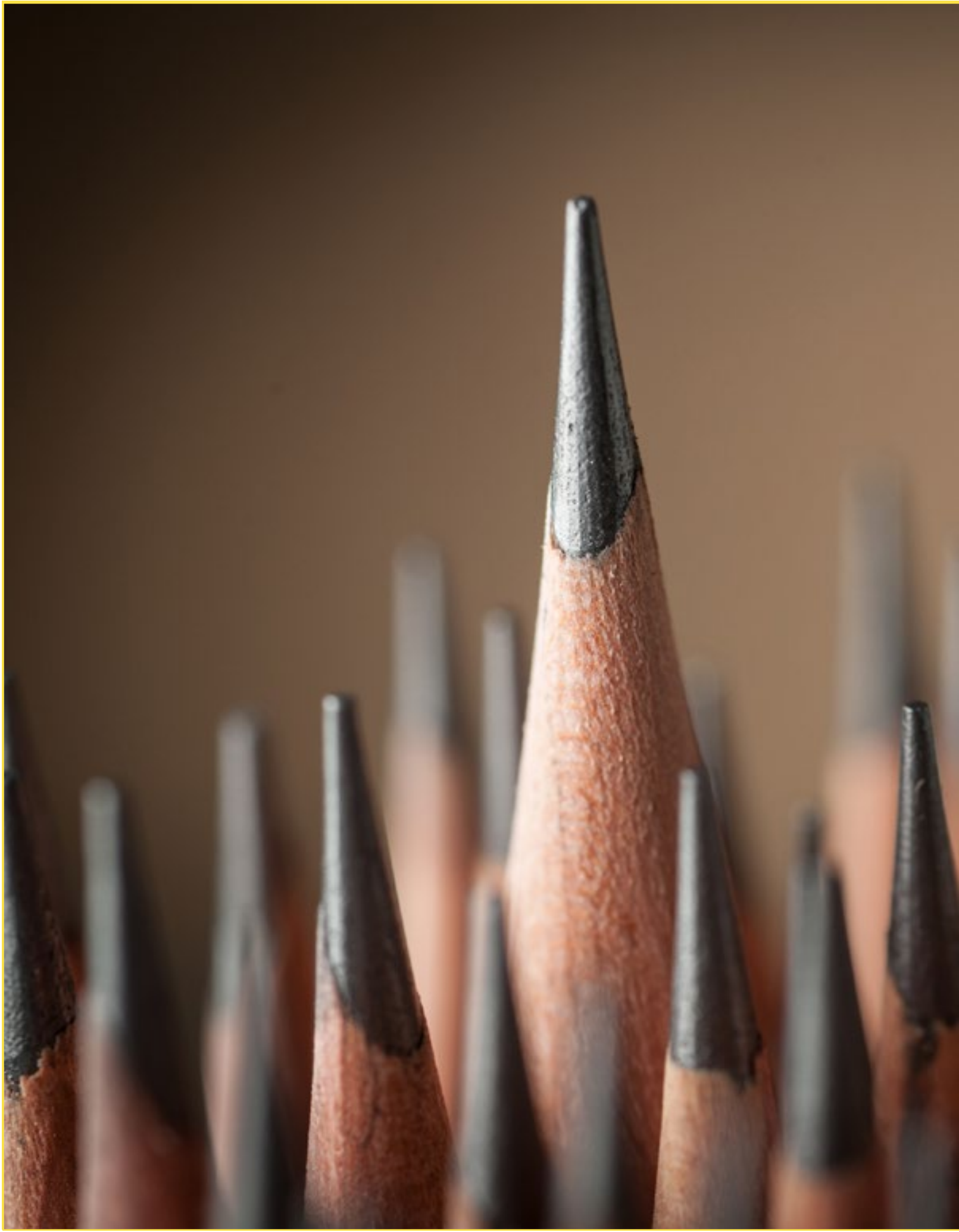
Naturally, strong network effects enjoyed by the dominant platforms limit contestability and competition between platforms of different sizes. It remains to be seen how externalities will affect costs of content curation and pricing of big platforms as opposed to smaller ones. The answer to this question will largely determine which market outcomes from the DSA materializes in reality.

05
FINAL REMARKS

We have argued that the updated liability rules introduced by the DSA may push platforms towards more intensive content screening to avoid overflow of notices. However, this will push the platforms' marginal costs of operations upwards, as well as their prices. This pass-through effect may take different forms in practice, depending on the type of a platform and adopted business model. Similarly, this may impact competition differently, depending on size asymmetries and how the platforms modify their prices as a response to increased moderation. In the specific case in which only big platforms increase their prices, the DSA may have a pro-competition effect, by allowing smaller platforms to attract more users, and more advertisers in turn, increasing their financial viability and reducing size asymmetries.
Even if we have tried to explore some competition effects deriving from the DSA, a more in-depth analysis of the intersection between the DSA and DMA would be, in our opinion, extremely interesting and needed. For instance, the DMA links in a number of ways with the above discussion of competition effects. As an example, the DMA attempts to provide more market contestability by implementing an asymmetric prohibition for gatekeeper platforms to pool data across many services. Other obligations included in the DMA may have similar expected effects on competition.

Similarly, other recent policy initiatives in the digital domain, such as the GDPR and the Data Act also link with the DSA in mitigating the excessive data extraction from the users. In the case of the Data Act, measures promoting data sharing could have a direct effect in reducing the cost of content moderation. This can be the case if increased access to data would allow the creation larger and more curated databases which could be used to improve prediction accuracy by smaller platforms to compensate their disadvantages from weaker network effects.

We have argued that the updated liability rules introduced by the DSA may push platforms towards more intensive content screening to avoid overflow of notices



OPERATIONALIZING THE REGULATION OF ONLINE CONTENT UNDER A DEMOCRATIC DEFICIT: THE DIGITAL SERVICES ACT

BY
DR. JOSEPH DOWNING

Senior Lecturer in International Relations and Politics, Aston University.

Debates about the divergent demands of freedom of expression on one hand and the need to regulate social media on the other have been reinvigorated in the past year with Elon Musk's acquisition of Twitter and the contending opinions of whether it will improve freedom of speech and transparency as he has promised,[2] or whether it will turn twitter into an "extremist ghetto" by offering a space for radical and xenophobic views.[3] However, little

2 Bradford Betz, "Elon Musk Teases Twitter Files on Free Speech Suppression: 'Public Deserves to Know,'" *FOXBusiness* (Fox Business, 2022), https://www.foxbusiness.com/politics/elon-musk-teases-twitter-files-free-speech-suppression-public-deserves-know.

3 Nesrine Malik, "Elon Musk's Twitter Is Fast Proving That Free Speech at All Costs Is a Dangerous Fantasy," *The Guardian*, November 28, 2022, https://www.theguardian.com/commentisfree/2022/nov/28/elon-musk-twitter-free-speech-donald-trump-kanye-west.

in the broader public, media or political discourse has considered that this promise is not necessarily in Musk's hands because neither he, nor Twitter, nor social media more generally, exist in a vacuum. National governments, and more recently, transnational governments, are increasingly seeking to regulate, and when required, impose sanctions on social media companies.

Europe is currently experiencing a renewed raft of social media regulations with the newly adopt Digital Services Act. This is significant because it demonstrates the European Union further intervening into the technology and digital arena. This Europeanisation of digital services legislation is muscular and sets out significant provisions for social media companies to be sanctioned for non-compliance and presents a range of issues for social media companies. In addition, the measures are unlikely to be a "silver bullet" solution to the range of problems presented by social media platforms. This intervention comes within a European context where American big tech has been blamed for many contemporary political and social ills, including fueling the rise of extremist politics[4] and spreading disinformation in the context of the COVID-19 pandemic.[5]

01

THE DIGITAL SERVICES ACT: KEY PROVISIONS

The Digital Services Act makes a range of provisions for the regulation of technology companies. These rules emerge in response to the rapid and widespread growth of digital services that further intrude into citizens and consumers daily lives. Against this context, the EU's intervention the "Digital Services Act" that aims to "create a safer digital space where the fundamental rights of users are protected"[6] and to "establish a level playing field to foster innovation, growth and competitiveness."[7] The scope of the Digital Services Act is vast. The rules specified by the act focus primarily on online intermediaries and platforms, which cover a huge area of online activity including marketplaces, social networks, and content sharing platforms in addition to "gatekeeper online platforms" that sit between businesses and consumers.[8] However, this article will focus on the potential issues that the Digital Services Act presents with a democratic deficit, the difficult nature of digital content moderation, and its inability to account for the agility of extremists to migrate to new platforms.

02

EUROPEANISATION AND THE DEMOCRATIC DEFICIT CREATED BY THE DIGITAL SERVICES ACT

The Digital Services Act is the landmark provision of the European Commission to regulate a range of digital services in the European space. However, given the multi- and trans-national nature of both the digital economy and the companies which operate within it, the bill effects digital services provision globally. Indeed, the European Commission openly promotes the Digital Services Act as having regulatory importance "both in the European Single Market and globally."[9] However, this fails to mention one of the key, and highly problematic aspects, of the Digital Services Act that gets directly at current debates about social media and free speech.

This is because the bill itself demonstrates that the transnational legislative ability of the European Commission can be subverted to pass legislation that is defeated at the national level. Here, the Digital Services Act demonstrates a questionable angle to the process of Europeanisation. Similar legislation was defeated by France's Supreme

4 *How Jokes Won the Election, The New Yorker,* January 23, 2017, *[Online] Available at*, ed. by E. Nussbaum, 2017; Zeynep Tufekci, "Opinion | YouTube, the Great Radicalizer - The New York Times," *The New York Times*, 2018, 5.

5 Wasim Ahmed and others, "COVID-19 and the 5G Conspiracy Theory: Social Network Analysis of Twitter Data," *Journal of Medical Internet Research*, 22.5 (2020), e19458, https://doi.org/10.2196/19458.

6 European Commission, "The Digital Services Act Package | Shaping Europe's Digital Future" https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

7 European Commission, "The Digital Services Act Package | Shaping Europe's Digital Future."

8 European Commission, "The Digital Services Act Package | Shaping Europe's Digital Future."

9 European Commission, "The Digital Services Act Package | Shaping Europe's Digital Future."

Court as posing a significant risk to freedom of expression.[10] This time around, the legislation has been heavily pushed by Macron as part of his assertion of the French position in Europe.[11] Macron using European legislative institutions as a means to promote and adopt regulations defeated by his own supreme court is problematic as a key principle of EU membership is that member states legislation follows EU legislation[12] and thus France will get regulations pushed onto it from above that it rejected at the member state level.

> ***This is because the bill itself demonstrates that the transnational legislative ability of the European Commission can be subverted to pass legislation that is defeated at the national level***

03

MODERATING CONTENT: UNPRECEDENTED OVERSIGHT AND OPERATIONAL ISSUES

A key provision of the Digital Services Act rests in the creation of European wide content moderation mechanisms that are separate from social media companies and thus gives the European Commission unprecedented oversight on what is, or is not, permissible discourse on social media. While this in itself is problematic, a further issue with this ambitious take on content moderation comes in the implementation phase of the legislation. This relates to a much broader set of issues related to all legislation and policy. This is the unpredictable process of implementation and operationalization. Thus, it is straightforward to promise a "safer digital space" and to "safeguard users rights" but far more difficult to actually deliver on such promises.

A key aim of the package is to tackle issues online with the spread of illegal content and misinformation. This has been a significant problem for some time, but two key issues emerge here. Firstly, the freedom of speech implications for imposing Europe wide standards on what is "illegal" content, decided on by unelected bureaucrats in Brussels sets a dangerous precedent. It was upon these grounds that the French supreme court defeated very similar measures formulated by the Macron government. The rules set out a framework for platforms to work with specialized "trusted flaggers"[13] to identify and remove content. However, training, retaining and the grounds upon which one will be "trusted" are ambiguous and reproduces many of the issues that platform moderation has already been criticized for in being unaccountable and expensive.[14] Indeed, the potential commercial burden for social media companies is enormous, and even the maximum fines of 6 percent of operating profits[15] (although actual fines are likely to be much smaller) could be seen as cheaper, and factored in as a business cost. This is not to mention the huge toll content moderation takes on human workers,[16] something which is likely to prove extremely problematic in terms of staff training and retention, as well as staff well-being.

10 EFF, "Victory! French High Court Rules That Most of Hate Speech Bill Would Undermine Free Expression," *Electronic Frontier Foundation*, 2020, https://www.eff.org/press/releases/victory-french-high-court-rules-most-hate-speech-bill-would-undermine-free-expression.

11 Laura Kayali, "Macron Goes after Online Platforms, Foreign 'Propaganda' Media," *POLITICO*, 2022 https://www.politico.eu/article/emmanuel-macron-online-platforms-foreign-propaganda-media.

12 European Commission, "Applying EU Law," *European Commission - European Commission* https://ec.europa.eu/info/law/law-making-process/applying-eu-law_en.

13 European Commission, "Questions and Answers: Digital Services Act," *European Commission - European Commission* https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348, accessed 29 November 2022.

14 Marietje Schaake & Rob Reich, "Election 2020: Content Moderation and Accountability," 6.

15 European Commission, *supra* note 13.

16 Jonathan Crossfield, "The Hidden Consequences of Moderating Social Media's Dark Side," *Content Marketing Institute*, 2019 https://contentmarketinginstitute.com/cco-digital/july-2019/social-media-moderators-stress, accessed November 29, 2022.

Complementing humans with algorithms and AI seem a "safer" and logical alternative. These algorithms have been criticized in the past for being too opaque and lacking transparency[17] and actually missing harmful content[18] because of the complex nuances of the text, image, video and audio-based nature of the social media landscape. The Digital Services Act specifies that these should be made transparent.[19] Again, this is not as straightforward as it may seem: algorithms also sort content to generate the revenue social media outlets need to survive,[20] and thus they are extremely commercially sensitive. Platforms invest huge amounts of money in the human and machine infrastructure to generate these complex models and are highly unlikely to be willing to openly offer up their trade secrets.

> ***This is because the bill itself demonstrates that the transnational legislative ability of the European Commission can be subverted to pass legislation that is defeated at the national level***

04

PLATFORM MIGRATION AND GETTING AROUND THE DIGITAL SERVICES ACT

The Digital Services Act sets out an extremely ambitious scope for the legislation to regulate a huge number of independent and international entities.

A final key issue that could significantly limit the effectiveness of the new legislation in its ability to combat fake news and hate speech comes from the remarkable agility of users themselves. Social media regulation and platform censorship aimed at taking down violent or hateful content is nothing new. However, users have shown significant agility to get around these attempts through platform migration. Both ISIS[21] and alt-right and conspiracy theory influencers[22] have demonstrated this by simply side-stepping censorship attempts and moving to apps like Telegram. The fact that many conspiracy theories thrive on ideas of victimhood and persecution by "the elite"[23] and a paranoia[24] that "they" are trying to stop "us" from discovering the truth is important is increased censorship attempts further give fuel to this fire. As social media platforms continue to proliferate and mushroom, questionable content will always be able to find a home.

17 Natalie Alana Ashton & Rowan Cruft, "Social Media Regulation: Why We Must Ensure It Is Democratic and Inclusive," *The Conversation*, 2022 http://theconversation.com/social-media-regulation-why-we-must-ensure-it-is-democratic-and-inclusive-179819, accessed November 22, 2022.

18 Schaake & Reich, *supra* note 14.

19 European Commission, *supra* note 13.

20 Sang Ah Kim, "Social Media Algorithms: Why You See What You See," *Georgetown Law Technology Review*, 2017 https://georgetownlawtechreview.org/social-media-algorithms-why-you-see-what-you-see/GLTR-12-2017.

21 Mitch Prothero, "ISIS Supporters Secretly Staged a Mass Migration from Messaging App Telegram to a Little-Known Russian Platform after the London Bridge Attack," *Insider*, 2019, https://www.insider.com/isis-sympathisers-telegram-tamtam-london-bridge-2019-12.

22 Richard Rogers, "Deplatforming: Following Extreme Internet Celebrities to Telegram and Alternative Social Media," *European Journal of Communication*, 35.3 (2020), 213–29, https://doi.org/10.1177/0267323120922066.

23 *Conspiracy Theories and the People Who Believe Them*, ed. by Joseph E. Uscinski (New York, NY: Oxford University Press, 2018).

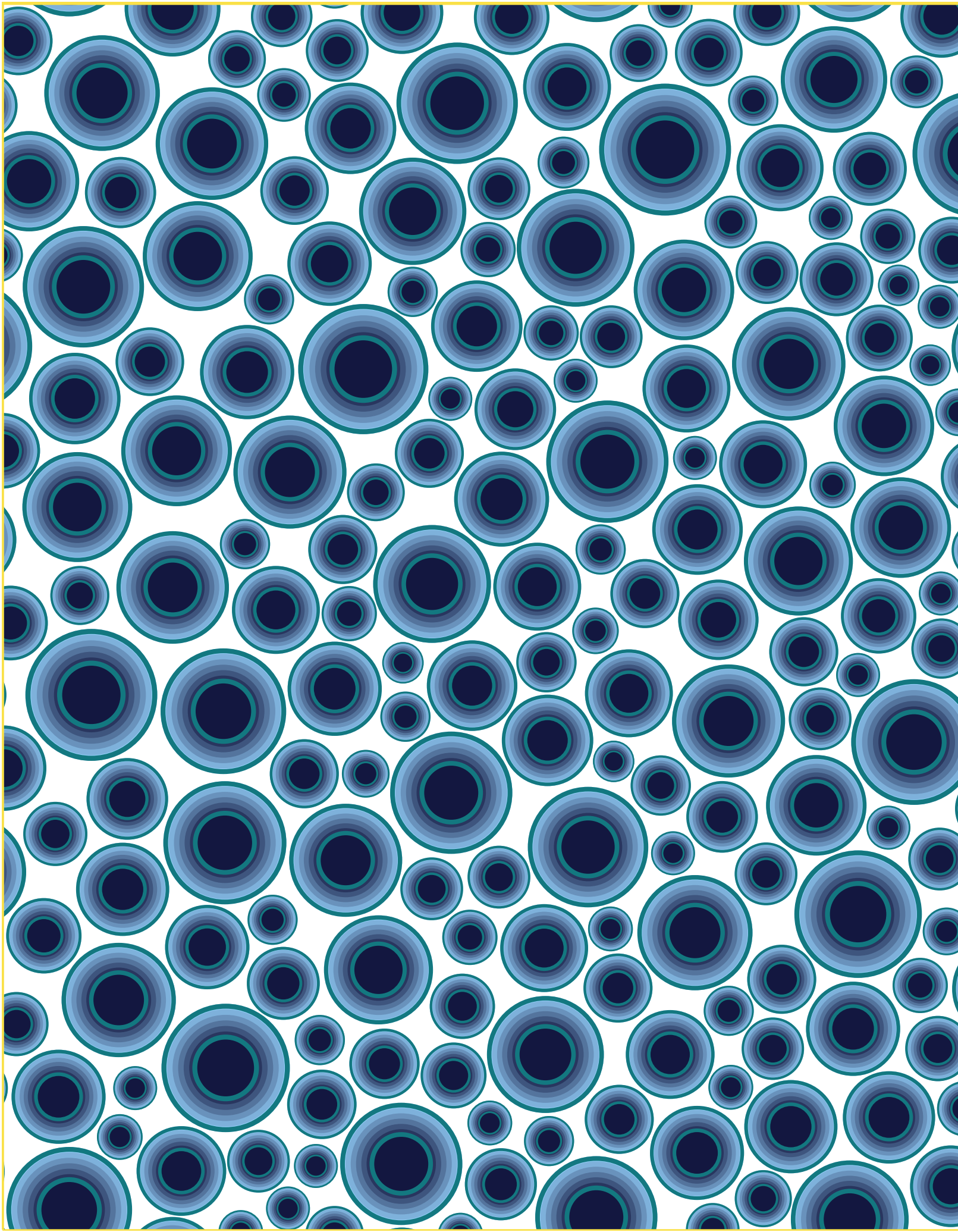
24 J. Eric Oliver & Thomas J. Wood, "Conspiracy Theories and the Paranoid Style(s) of Mass Opinion," *American Journal of Political Science*, 58.4 (2014), 952–66.

05

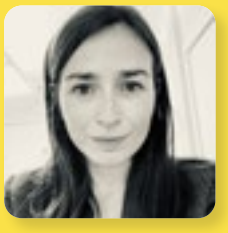
CONCLUSIONS ON THE DIGITAL SERVICES ACT: THE PARADOX OF REGULATION

Social media regulation is complex and problematic, but it is also difficult to imagine a situation in today's digital world where social media is unregulated. However, it is much easier for regulators to make promises than to either operationalist these or to gain compliance from large multinational companies. Also, Macron's push for more legislation at the European level after similar rules were defeated in France demonstrate a problematic aspect of Europeanisation and the democratic deficit where the commission is deciding how a member state should manage digital free speech by going over the head of the member states supreme court. Additionally content moderation has become an ever more contentious.

Social media regulation is complex and problematic, but it is also difficult to imagine a situation in today's digital world where social media is unregulated



THE DSA, DUE DILIGENCE & DISINFORMATION: A DISJOINTED APPROACH OR A RISKY COMPROMISE?



BY
KATIE PENTNEY

DPhil Candidate in Law, University of Oxford: katie.pentney@law.ox.ac.uk.

01 INTRODUCTION

The long-awaited Digital Services Act ("DSA") was finally signed into law by the European Union on October 19, 2022, after lengthy drafting and hard-fought negotiation processes.[2] The flagship Regulation harmonises existing rules applicable to internet intermediaries and imposes new transparency and accountability requirements on online platforms, as well as heightened due diligence obligations on so-called "very large online platforms" ("VLOPs")

2 *Regulation (EU) 2022/2065 of the European Parliament and the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)* ("**DSA**"), Official Journal of the European Union L 277, Vol 65 (27 October 2022).

like Facebook, Google (YouTube) and Twitter.[3] The stated objective of the DSA is to ensure a "safe, predictable and trusted online environment" by addressing the dissemination of illegal content online, as well as "the societal risks that the dissemination of disinformation or other content may generate."[4]

This was a long time coming for those concerned about the well-documented proliferation of illegal and harmful content online. The celebrations were, however, short-lived (or at least dampened): the day after the DSA was published in the EU Official Journal, marking the end of its adoption process (and the start of the 20-day countdown until its entry into force), Elon Musk completed his acquisition of Twitter. The takeover sparked concern that the self-proclaimed "free speech absolutist" would roll-back existing content moderation practices and allow conspiracy theories, disinformation and hate speech to proliferate unabated on the platform.[5] While it is still early days, at least some of these concerns appear to be well-founded: in the 48 hours following the takeover, Twitter's Head of Safety & Integrity tweeted that "a small number of accounts post[ed] a ton of Tweets that include slurs and other derogatory terms," before adding "To give you a sense of scale: More than 50,000 Tweets repeatedly using a particular slur came from just 300 accounts."[6] The entire human rights team at Twitter has since been fired,[7] and Musk himself has since tweeted, and then deleted, an unfounded conspiracy theory regarding the attack on US Speaker of the House Nancy Pelosi's husband, Paul.[8] Before he had deleted the tweet, it had been retweeted 24,000 times and received more than 86,000 likes.[9]

The Twitter takeover by a self-proclaimed "free speech absolutist" illustrates the potential pitfalls of the EU's chosen approach of "deferential regulating" – through which it imposes due diligence obligations on the likes of Twitter, Facebook and other VLOPs operating within the EU, but affords significant deference and leeway for internal decision-making by these online platforms. The battles to be waged are (somewhat ironically) best illustrated by a Twitter exchange between Musk and the EU's Internal Market commissioner, Thierry Breton. Upon finalizing his acquisition, Musk tweeted, "the bird is freed"; shortly thereafter, Breton retorted (in Tweet form): "In Europe, the bird will fly by our [EU] rules."[10]

"This was a long time coming for those concerned about the well-documented proliferation of illegal and harmful content online

3 DSA, Recital 9. "VLOP" means, for the purposes of the Regulation, online platforms "which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as [VLOPs…] pursuant to paragraph 4" (DSA, Article 33(1)). See also Natascha Just, *The Taming of Internet Platforms – A Look at the European* Digital Services Act, CPI TechREG CHRONICLE (June 15, 2022), https://www.competitionpolicyinternational.com/the-taming-of-internet-platforms-a-look-at-the-european-digital-services-act/.

4 DSA, *supra*, Recital 9.

5 Dan Milmo & Alex Hern, *Twitter takeover: fears raised over disinformation and hate speech*, THE GUARDIAN, Oct. 28 2022, https://www.theguardian.com/technology/2022/oct/28/twitter-takeover-fears-raised-over-disinformation-and-hate-speech; Guardian staff and agencies, *Elon Musk declares Twitter "moderation council" – as some push the platform's limits*, THE GUARDIAN, Oct. 29, 2022 https://www.theguardian.com/technology/2022/oct/28/elon-musk-twitter-moderation-council-free-speech.

6 Yael Roth, Twitter, https://twitter.com/yoyoel/status/1586542283469381632.

7 Kate Conger, Ryan Mac & Mike Isaac, *Confusion and Frustration Reign as Elon Musk Cuts Half of Twitter's Staff*, NEW YORK TIMES, Nov. 4, 2022, https://www.nytimes.com/2022/11/04/technology/elon-musk-twitter-layoffs.html; Sam Levin, Richard Luscombe & Graeme Wearden, *Twitter layoffs: anger and confusion as multiple teams reportedly decimated – as it happened*, THE GUARDIAN, Nov. 5, 2022 https://www.theguardian.com/business/live/2022/nov/04/twitter-sued-layoffs-sizewell-nuclear-plant-uk-recession-us-jobs-business-live#:~:text=The%20human%20rights%20team%20has,in%20Ukraine%2C%20Afghanistan%20and%20Ethiopia.

8 Julianne McShane, *Elon Musk, new owner of Twitter, tweets unfounded anti-LGBTQ conspiracy theory about Paul Pelosi attack*, NBC NEWS, Oct. 30, 2022 https://www.nbcnews.com/news/us-news/elon-musk-new-owner-twitter-tweets-unfounded-conspiracy-theory-paul-pe-rcna54717.

9 *Id.*

10 Thierry Breton, Twitter, https://twitter.com/ThierryBreton/status/1585902196864045056?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1585902196864045056%7Ctwgr%5E1f36754db79be083c89e8995b46b97d9fff8f4ff%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.theguardian.com%2Ftechnology%2F2022%2Foct%2F28%2Ftwitter-takeover-fears-raised-over-disinformation-and-hate-speech.

This article offers some preliminary thoughts on the likelihood that these "EU rules" will achieve their stated aims of ensuring a "trusted online environment," generally, and addressing the societal risks of online disinformation, specifically. While the DSA imposes transparency and other requirements on all internet intermediaries, the focus of this article is on the heightened due diligence framework imposed on VLOPs, in particular. It proceeds in two parts. First, I provide a brief overview of the key features of the risk-based due diligence framework, as well as some of the issues they raise. Second, I offer some reflections on the newly enacted DSA's disjointed approach to disinformation, specifically, and the enforcement difficulties which seem poised to lie ahead, if Musk's recent acquisition of Twitter is any indication.

02

THE DSA'S HEIGHTENED DUE DILIGENCE FRAMEWORK

The EU is not alone in expressing concerns about the societal risks that the proliferation of disinformation online may pose. To the contrary, such concerns are well documented and multifaceted, particularly when it comes to elections, public health emergencies or foreign invasions. The World Health Organization ("WHO") has decried the "infodemic" that has accompanied – and at times, worsened – the COVID-19 pandemic: indeed, WHO notes that "In the first 3 months of 2020, nearly 6 000 people around the globe were hospitalized because of coronavirus misinformation" and during this same period, "research say at least 800 people may have died due to misinformation related to COVID-19."[11] Carley notes that as COVID-19 spread around the word, so too did "an epidemic of disinformation and misinformation":

> Estimates suggest that there have been hundreds of thousands of distinct disinformation stories with respect to the pandemic. These stories included the innocuous—such as due to the lockdown pollution was lower in Venice and the swans and dolphins returned to the canals. Other stories were lethal—such as drink bleach to cure yourself of COVID-19. Still other disinformation stories were woven together to form larger conspiracy theories—such as Bill Gates invented the SARS-CoV-2 virus and the vaccine […].[12]

Beyond COVID-19, the impact of so-called "information disorder"[13] on elections in the US and France and on referenda in the United Kingdom and beyond has raised concerns about the effects of disinformation, misinformation and malinformation in public discourse and democratic pro-

11 World Health Organization, Fighting misinformation in the time of COVID-19, one click at a time (April 27, 2021) https://www.who.int/news-room/feature-stories/detail/fighting-misinformation-in-the-time-of-covid-19-one-click-at-a-time, citing Md Saiful Islam et al, *COVID-19-Related Infodemic and Its Impact on Public Health*, 103 Am. J. Trop. Med. Hyg. 4, 1621 (2020). See also European Commission, *Tackling coronavirus disinformation* https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_en.

12 Kathleen Mary Carley, *A Political Disinfodemic*, in COVID-19 DISINFORMATION: A MULTI-NATIONAL, WHOLE OF SOCIETY PERSPECTIVE (Rita Gill & Rebecca Gooslby eds, 2022) 1, 2.

13 This is the umbrella term used by Claire Wardle and Hossein Derakhshan to refer to three subcategories: disinformation, misinformation and malinformation. Claire Wardle & Hossein Derakhshan, *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe, DGI(2017)09 (2017) https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

cesses.[14] Similarly, the Russian state (and its affiliates) have weaponized disinformation to justify and perpetuate the war on Ukraine.[15] Tim Wu notes the distorting effect of disinformation campaigns, which have "rapidly become the speech control technique of choice in the early 21st century."[16] He posits that "disinformation techniques are a serious threat to the functioning of the marketplace of ideas and democratic deliberation, and therefore, it has fallen upon other institutions—especially the press and sometimes others—to fight them."[17]

It is against this backdrop that the EU has adopted the DSA – its flagship regulation imposing requirements on internet intermediaries to join the fight against the spread of illegal and harmful content online. For present purposes, the key feature of interest is the DSA's imposition of a heightened due diligence framework on VLOPs in light of their scale, reach and importance in "facilitating public debate, economic transactions and the dissemination to the public of information, opinions and ideas and in influencing how recipients obtain and communicate information online."[18] There are three main pillars of the heightened due diligence approach: (i) a systemic risk assessment; (ii) mitigation of identified systemic risks; and (iii) an annual independent audit requirement.[19] Each of these pillars is reviewed in turn.

"It is against this backdrop that the EU has adopted the DSA – its flagship regulation imposing requirements on internet intermediaries to join the fight against the spread of illegal and harmful content online

A. The Risk Assessment

The first and foundational element of the heightened due diligence framework is the requirement that VLOPs undertake a risk assessment in which they "diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use of their services."[20] The risk assessment must be "specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability" and must include the following identified "systemic risks":

> (a) the dissemination of illegal content through their services;
> (b) any actual or foreseeable negative effects for the exercise of fundamental rights, including human dignity, respect for private and family life, data protection, freedom of expression, and non-discrimination;
> (c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security; and
> (d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.[21]

This provision indicates the two strands of content identified to pose a "risk" and therefore targeted by the Regulation: illegal content, on the one hand, and "lawful but awful" content, on the other. However, while one of the stated objectives of the DSA is to address the "societal risks that the dissemination of disinformation or other content may generate," disinformation is not included as a specific systemic risk of which VLOPs must be aware. This may be because disinformation traverses the systemic risks iden-

14 See generally Max Bader, *Disinformation in Elections*, 29 Sec. and Hum. R. 24 (2018); SANDRINE BAUME ET AL. (eds) MISINFORMATION IN REFERENDA (1st ed., 2021).

15 Olivia B Waxman, *What Putin Gets Wrong About 'Denazification' in Ukraine*, TIME, Mar. 3, 2022, https://time.com/6154493/denazification-putin-ukraine-history-context/; Brian Klaas, *Vladimir Putin Has Fallen Into the Dictator Trap*, THE ATLANTIC, Mar. 16, 2022) https://www.theatlantic.com/ideas/archive/2022/03/putin-dictator-trap-russia-ukraine/627064/. See also *Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide (Ukraine v. Russian Federation)*, Order of the International Court of Justice (March 23, 2022) §§ 28-47.

16 Tim Wu, *Disinformation in the Marketplace of Ideas*, 51 *Seton Hall L.R.* 169, 169 (2020).

17 *Id.* 170.

18 DSA, *supra*, recital 75. See generally DSA, Section 5.

19 For a more in-depth review of the (draft) provisions, see Tarlach McGonagle & Katie Pentney, *From risk to reward? The DSA's risk-based approach to disinformation* in UNRAVELLING THE DIGITAL SERVICES ACT PACKAGE (IRIS *Special*, European Audiovisual Observatory, M. Cappello ed., 2021) 43.

20 DSA, *supra*, Article 34(1).

21 *Id*.

tified – from negatively affecting civic discourse and electoral processes, to public security, to protection of public health. Yet it is a notable divergence with the approach to "illegal content," which is explicitly identified as a systemic risk, and included without further elaboration of particular *kinds* of illegal content.[22] But there is very little guidance or direction about what kinds of "actual or foreseeable negative effects" on fundamental rights, civic discourse/elections, public security, or protection of public health VLOPs would fit the bill, what threshold must be reached in order for the risk to be "systemic," or how proximate such effects must be. Read broadly, this provision could capture much of what happens in the online ecosystem, given the scope of the fundamental rights included in the Regulation and the breadth and vagueness of the systemic risks listed. This could have serious repercussions for the flow of information and ideas online – particularly those which might "offend, shock or disturb"[23] – when read together with the second element of the due diligence framework: the requirement of mitigation.

> ***This provision indicates the two strands of content identified to pose a "risk" and therefore targeted by the Regulation***

B. The Mitigation of Risk Requirement

The second pillar is the requirement that VLOPs put in place "reasonable, proportionate and effective mitigation measures" which are "tailored to the specific systemic risks identified" and "with particular consideration to the impacts of such measures on fundamental rights."[24] The Regulation sets out a list of illustrative examples of such mitigation measures, including adapting the design, features or functioning of their platforms, taking awareness-raising measures to give users more information, and ensuring that false or inauthentic information "is distinguishable through prominent markings when presented on their online interfaces."[25] While the Regulation requires mitigation measures that are tailored to the systemic risks identified, it once again defers to VLOPs with respect to how best to do so, and provides little guidance about what would fulfill the qualitative requirements that the measures be reasonable, proportionate and effective.

The more generalized mitigation measures are supplemented by the "crisis response mechanism" particularized in Article 36, which is triggered (somewhat unhelpfully) and imprecisely "[w]here a crisis occurs."[26] The preamble notes that a crisis "should be considered to occur when extraordinary circumstances occur that can lead to a serious threat to public security or public health in the Union or significant parts thereof" and further provides that such crises "could result from armed conflicts or acts of terrorism, […] natural disasters […] as well as from pandemics and other serious cross-border threats to public health."[27] The crisis response mechanism was a late addition to the DSA: it did not appear in earlier drafts, but was added in response to the Russian war on Ukraine.[28] It was the subject of significant criticism from civil society organizations when it was introduced late in the process on the basis that it was "an overly broad empowerment of the European Commission to unilaterally declare an EU-wide state of emergency" and would "enable far-reaching restrictions of freedom of expression and of the free access

22 Recital 12 does provide that "the concept of 'illegal content' should be defined broadly to cover information relating to illegal content, products, services and activities." (DSA, *supra*, Recital 12). It further states that "Illustrative examples include the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking" and so on.

23 *Handyside v. United Kingdom*, App no 5493/72 (Plenary, December 7, 1976) § 49.

24 DSA, *supra*, Article 35(1).

25 *Id*.

26 DSA, *supra*, Article 36.

27 *Id.*, Recital 91.

28 38 organizations called on DSA negotiators to "stop negotiating outside their respective mandates and respect the democratic process of the EU": see Press Release, European Digital Rights (**EDRi**), A new crisis response mechanism for the DSA (April 12, 2022) https://edri.org/our-work/public-statement-on-new-crisis-response-mechanism-and-other-last-minute-additions-to-the-dsa/. See also Press Release, Access Now, Civil society to EU: don't threaten rights with last-minute 'crisis response mechanism' in DSA (April 13, 2022) https://www.accessnow.org/crisis-response-mechanism-dsa/.

to and dissemination of information in the Union."[29] Some of the specific concerns were addressed in the Regulation as adopted, including requiring that the actions taken in line with this provision are "strictly necessary, justified and proportionate, having regard in particular to the gravity of the serious threat referred to in paragraph 2, the urgency of the measures and the actual or potential implications for the rights and legitimate interests of all parties concerned."[30]

C. The Independent Audit

The third and final pillar of the due diligence scheme is the independent audit, to which VLOPs shall be subjected on an annual basis to assess compliance with the transparency and due diligence obligations set out in Chapter III and with any commitments they've undertaken pursuant to codes of conduct and crisis protocols.[31] The audit must result in a report which includes an opinion on whether the VLOPs complied with their obligations and commitments.[32] Where the opinion is not "positive," the report must also include operational recommendations on the specific measures to achieve compliance and the recommended timeframe for doing so.[33] The report may be redacted as necessary to protect confidential information.[34] Upon receipt of the audit report, providers of VLOPs must "take due account of the operational recommendations addressed to them with a view to take the necessary measures to implement them."[35] They have one month from receiving the recommendations to adopt an "audit implementation report" setting out implementation measures.[36] Given the scope of the obligations set out in the DSA, it may be impractical – if not impossible – for VLOPs to respond to the audit report within this timeframe, or to do so in more than a cursory way. Moreover, while this third and final piece brings in the independent oversight needed to peer behind the veil, the requirement that VLOPs "take due account of" the recommendations provided "*with a view to* take the necessary measures to implement them" seems to leave significant leeway to VLOPs about how quickly, and how thoroughly, they must make changes.

"The third and final pillar of the due diligence scheme is the independent audit, to which VLOPs shall be subjected on an annual basis to assess compliance with the transparency and due diligence obligations set out in Chapter III and with any commitments they've undertaken pursuant to codes of conduct and crisis protocols

D. A Disjointed Approach or a Risky Compromise?

The risk-based approach thus attempts to balance the competing interests and calls from interested sectors of the population, including the public and regulators, civil society, and online platforms. It responds to regulators' (and members of the public's) desire to combat the proliferation of harmful and illegal content online by requiring VLOPs to play ball in addressing the problem. At the same time, it takes on board the concerns raised by civil society organizations within (and beyond) Europe relating to the lack of transparency about how content moderation decisions are made by large online platforms like Facebook, Twitter and Google (YouTube) and the absence of oversight as to whether such decisions comply with fundamental rights under the EU Charter.[37] Finally, the approach aims to appease the tech sector by deferring to online platforms and affording significant leeway in identifying the systemic risks that most affect their services and users, and selecting

29 EDRi, *Public Statement: ON NEW CRISIS RESPONSE MECHANISM AND OTHER LAST MINUTE ADDITIONS TO THE DSA* (April 12, 2022) https://edri.org/wp-content/uploads/2022/04/EDRi-statement-on-CRM.pdf.

30 DSA, *supra*, Article 36(3).

31 *Id.*, Article 37.

32 *Id.*, Article 37(3) and (4). The audit opinion must indicate whether it is "positive," "positive with comments" or "negative" (per Article 37(4)(g).

33 *Id.*, Article 37(4)(h).

34 *Id.*, Article 37(2).

35 *Id.*, Article 37(6).

36 *Id*.

37 See, for instance, the Santa Clara Principles on Transparency and Accountability in Content Moderation, https://www.santaclaraprinciples.org/; Rikke Frank Jørgensen (ed.), HUMAN RIGHTS IN THE AGE OF PLATFORMS (2019).

the best options to mitigate them. But how this negotiated compromise will work in practice remains a significant question mark, particularly in responding to the proliferation of so-called "lawful but awful" content like disinformation. The next section offers some broader context about how the DSA came to address disinformation at all and outlines a few of the lingering questions that remain in respect of implementing and enforcing the risk-based approach as against disinformation.

03

IMPLEMENTING & ENFORCING THE RISK-BASED APPROACH *VIZ.* DISINFORMATION

The DSA's approach to disinformation can be described as ambiguous, uneasy or disjointed – terms that legislative drafters should seek to avoid. Whatever qualifier one chooses, the upshot is that VLOPs' internal compliance and human rights teams are left in the unenviable position of having to make sense of these newly-imposed, but imprecisely drafted, requirements in rather short order.

For starters, the term "disinformation" is used, but nowhere defined, in the Regulation. In light of the variation in definitions – within and beyond the EU – this seems a glaring oversight (at best) or an intentional omission (at worst).[38] In either case, it leaves online platforms in the unenviable position of having to sort it out for themselves, which may result in inconsistent approaches between platforms, and over-regulation of content, with all of the corresponding human rights issues that entails.[39] In addition, each of the thirteen references to "disinformation" are found in the DSA's preambular recitals, rather than its substantive provisions setting out the risk-based approach, and many are sandwiched between the companion focuses of "illegal content" (which is defined) and "other societal risks" (which appears to be a catch-all for the negative impacts of the online ecosystem in the offline realm).[40]

"The DSA's approach to disinformation can be described as ambiguous, uneasy or disjointed – terms that legislative drafters should seek to avoid

Of course, the DSA is but one piece of a broader and complex regulatory and policy landscape governing disinformation within the EU. Though the DSA's stated objective refers to the proliferation of disinformation, the Regulation is not primarily concerned with disinformation: it operates in parallel with other (more targeted) efforts to combat disinformation, including co-regulatory efforts like the Strengthened Code of Practice on Disinformation 2022, which was negotiated alongside the DSA and adopted earlier this year.[41] Whether the EU's intention was to take a soft-touch with the DSA to allow the 2022 Strengthened Code of Practice to do the heavy lifting in respect of disinformation remains unclear. However, the resulting "piecemeal" approach to disinformation has been the subject of criticism,[42] and its omission from the "systemic risks" identified in Article 34 leaves lingering uncertainty about whether and to what extent the DSA enables or requires VLOPs to address its spread on their platforms, separate and apart from any obligations they have agreed to under

38 For the definitional dilemmas, see McGonagle & Pentney, *supra*, 44-47; Ronan Ó Fathaigh, Natali Helberger & Naomi Appelman, *The Perils of Legally Defining Disinformation*, 10 Internet Pol. Rev. 4, 1-25 (2022).

39 See generally Jørgensen (2019), *supra*; Jillian C. York, SILICON VALUES: THE FUTURE OF FREE SPEECH UNDER SURVEILLANCE CAPITALISM (2021).

40 See e.g. DSA, *supra*, Recitals (2) and (9). Recital 84, by contrast, refers to disinformation within the broader category of "misleading or deceptive content." Tambini has characterized the DSA as a "co-regulatory backstop" for disinformation: Damien Tambini, *Media policy in 2021: As the EU takes on the tech giants, will the UK*? LONDON SCHOOL OF ECONOMICS, Jan. 12, 2021 https://blogs.lse.ac.uk/medialse/2021/01/12/media-policy-in-2021-as-the-eu-takes-on-the-tech-giants-will-the-uk/.

41 Strengthened Code of Practice on Disinformation (June 2022), https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

42 Ethan Shattock, *Self-regulation 2:0? A critical reflection of the European fight against disinformation* (Harvard Kennedy School Misinformation Review, May 31, 2021) https://misinforeview.hks.harvard.edu/article/self-regulation-20-a-critical-reflection-of-the-european-fight-against-disinformation/.

the 2022 Strengthened Code of Practice on Disinformation.[43]

The disjointed approach to disinformation – perhaps best illustrated by the preamble's frequent references to the problem and the total exclusion of the concept from the DSA's substantive provisions – may in fact be a by-product of the hard-fought drafting and negotiation processes within the EU. Indeed, the question of whether disinformation ought to be addressed by the DSA at all was a fundamental issue throughout the negotiations. The Committee on Civil Liberties, Justice and Home Affairs of the European Parliament ("LIBE Committee") thought not: its Draft Opinion, released in May 2021, put forward a number of amendments, most crucially for present purposes the deletion of the provisions setting out the risk-based due diligence approach (discussed above).[44] The LIBE Committee justified these amendments on the basis that they were necessary to protect freedom of expression and to ensure the DSA was tailored to address the dissemination of *illegal* rather than *harmful* content.[45] The LIBE Committee expressed concern that the requirements in Article 26 (setting out the risk-based approach) went "far beyond illegal content where mere vaguely described allegedly "negative effects" are concerned."[46] Similar concerns were raised regarding the independent audit requirements set out in Article 28.[47] The LIBE Committee's suggested amendments illustrate the disconnect between the broad aims sought to be achieved by the drafters, and the more circumscribed scope preferred by the LIBE Committee, which would have effectively removed from the DSA's purview "lawful but awful" speech, such as disinformation.

Where, then, does that leave VLOPs when it comes to identifying and mitigating the risks posed by disinformation? Several points appear (relatively) clear even at this early stage. First, the DSA is focused on particular *contexts* rather than specific *content*: the proliferation of disinformation that has actual or foreseeable negative effects on civic discourse, electoral processes, public security or the protection of public health must be included in VLOPs' risk assessments and mitigated accordingly. As a threshold, this at least appears straightforward. However, from there, issues arise: how can one establish that particular (knowingly false and intentionally shared) content has had actual negative effects on public health or civic discourse? What level of causation is necessary, or sufficient, for VLOPs to take action? What level of foreseeability is required in order to identify, assess and mitigate a systemic risk posed by disinformation in relation to electoral processes? Is the proliferation of disinformation in previous elections sufficient to foresee a similar risk arising in future? And even where such a risk has been identified in the risk assessment, how can it be mitigated in a manner that accords sufficient protection for political speech or debates of questions of public interest, for which few restrictions are permitted?[48] More broadly, will the heightened due diligence framework have any (micro) effect on specific disinformation that is shared on the platforms, or will it simply result in broader design and "system" changes on a macro level, for instance changes to algorithmic content moderation at scale?

> ***Of course, the DSA is but one piece of a broader and complex regulatory and policy landscape governing disinformation within the EU***

Finally, and most fundamentally, a large question remains about whether the deference afforded to VLOPs in identifying, analysing, assessing and mitigating systemic risks stemming from the design or functioning of their service is a gamble that will pay off. Elon Musk's Twitter acquisition, and subsequent firing of the entire human rights team, casts this in stark relief, but the problem goes deeper still. Facebook, Twitter and Google (YouTube) are based in the US, with a free speech tradition that diverges significantly from

43 For instance, signatories agreed to take action in "demonetising the dissemination of disinformation; ensuring the transparency of political advertising; empowering users; enhancing the cooperation with fact-checkers; and providing researchers with better access to data." (2022 Strengthened Code of Practice, *supra*).

44 Committee on Civil Liberties, Justice and Home Affairs for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825) (May 19, 2021) Amendments 21-24, 28, 29, 91-93, https://www.europarl.europa.eu/doceo/document/LIBE-PA-692898_EN.pdf.

45 *Id*. Amendment 91, "Justification" p. 64/84.

46 *Id*. pp. 64-65/84.

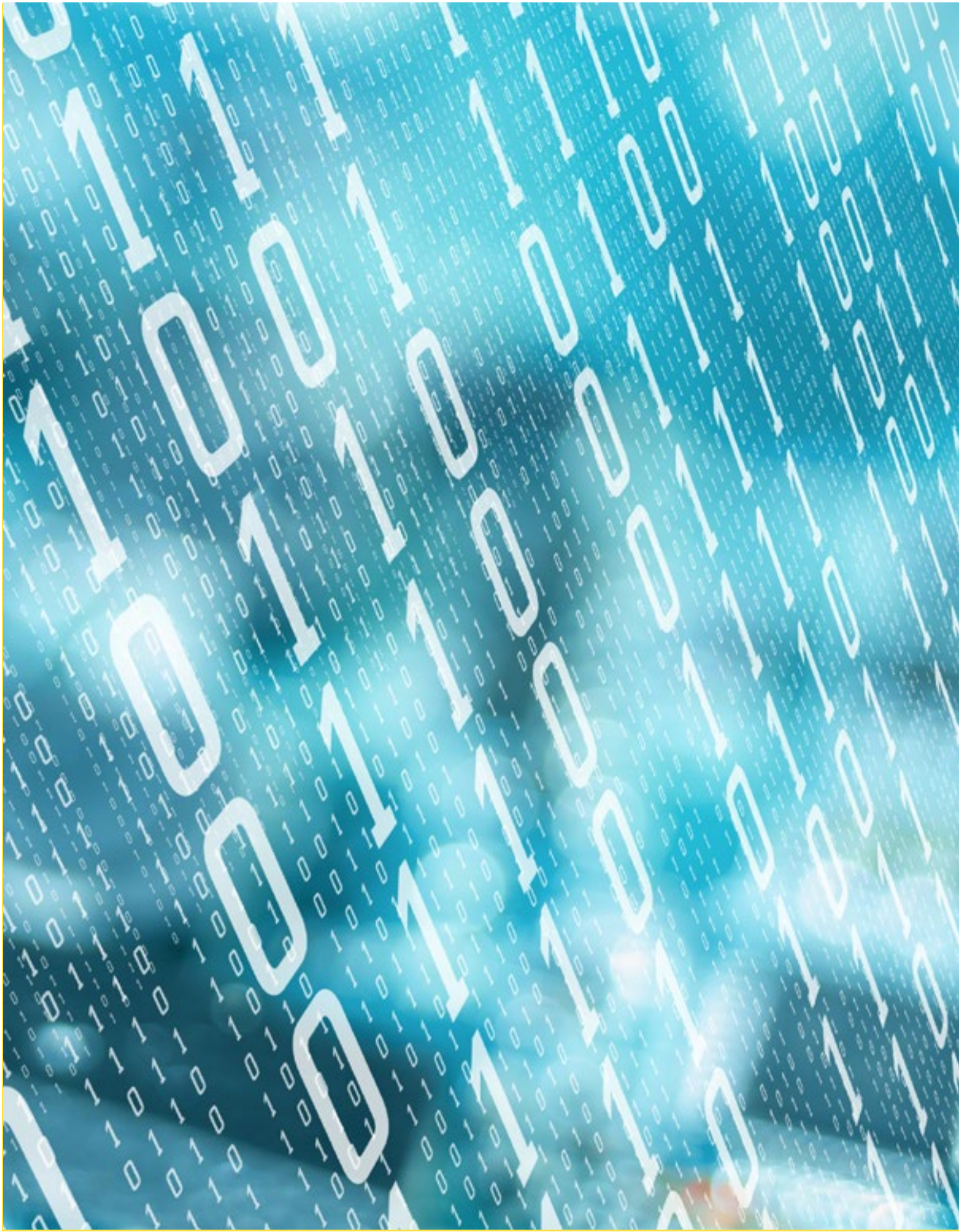
47 *Id*. Amendment 102, pp. 69-70/84.

48 *Castells v. Spain*, App no 11798/85 (Chamber, April 23, 1992) § 43; *Wingrove v. United Kingdom*, App no 17419/90 (Chamber, November 25, 1996) § 58.

that of the EU.[49] Leaving it to the likes of Elon Musk and Mark Zuckerberg (or their chosen executives) to not only balance competing rights and interests, but to *decide what to weigh on the scales*, may prove an unwise choice. It may also severely limit the potential of the DSA to achieve its stated objective of ensuring a safe, predictable and trusted online environment. Just how freely the bird will fly in Europe – and how far the EU succeeds in clipping VLOPs' wings – remains to be seen.

> ***Elon Musk's Twitter acquisition, and subsequent firing of the entire human rights team, casts this in stark relief, but the problem goes deeper still***

49 See e.g. Jared Schroeder, *Meet the EU Law That Could Reshape Online Speech in the U.S*, SLATE, Oct. 27, 2022 https://slate.com/technology/2022/10/digital-services-act-european-union-content-moderation.html; Mark Scott, *Musk vs. Europe: The upcoming battle over free speech*, POLITICO, April 26, 2022 https://www.politico.eu/article/elon-musk-europe-online-content-free-speech/.



ALGORITHMIC SEARCH AND RECOMMENDER SYSTEMS IN THE DIGITAL SERVICES ACT

BY OLIVER BUDZINSKI

& MADLEN KARG

Oliver Budzinski is Professor of Economic Theory and the Director of the Institute of Economics at Ilmenau University of Technology, Germany. Madlen Karg is Research and Teaching Fellow at the Department of European Law and Public International Law at the University of Innsbruck, Austria.

01 INTRODUCTION

Among the various phenomena of the world of digital services, the channeling of users' attention to a pre-selection of goods through algorithmic search and recommender systems (ASRS) represents one of the most important issues. On the one hand, information overload on the internet requires some pre-selection, on the other hand, the power of the algorithm raises doubts and fears about their impact on competition and society. The EU Digital Services Act (DSA) applies a cautious regulation

of ASRS. In order to assess its adequacy from a law and economics perspective (sections 3 and 4), we first take a look into the economics behind these systems (section 2).[2]

02
THE ECONOMIC ROLE OF (ALGORITHMIC) SEARCH AND RECOMMENDATION SYSTEMS

A. Information Overload, Search Costs, and Decision-Making

Digital markets are usually characterized by information overload since the amount of goods and contents offered on the internet in general and on specific online marketplaces (à la Amazon), audio and video streaming services (e.g. Spotify, YouTube, Netflix, etc.) or in App Stores regularly exceeds the information processing capacities of users. Therefore, it is necessary that online services provide a preselection of the available items to users. Only this artificial reduction of the perceivable range of supply allows users to perform a rational consumption choice among commodities, services, and contents.

This pre-selection of contents is usually based on search and recommendation systems, often automatized through algorithms. In the case of search services, the initiative is with the user who provides a search inquiry and receives so-called hits as a response from the system. These hits are not presented in a random order; instead, they are ordered with the goal to provide the best fitting response first. As such, search systems include an element of recommendation through the immanent ranking of the hits. Pure recommendation systems proactively address the users and suggest to them further items that they may like to consume. The wide range of systems include "other users also bought"-style recommendations up to auto-play versions where the next recommended audio or video stream automatically starts after the chosen one has ended. Like the ranking in search systems, recommendation systems try to offer a best next choice option to the user and do not present items in a random order.

The ranking of search results and recommendations influences the choice of the users. The top-ranking positions receive significantly more attention than the items further down the order. Empirical studies confirm that most users only perceive the first 4-5 search hits or recommendation items and, thus, de facto only choose among these contents, commodities, and services.[3] The theoretical explanation refers to the scarcity of cognitive resources and transaction costs of choice. Rational users will not use unlimited cognitive resources to search for and choose among goods, especially not in situations of information overload. Instead, they stop the search and choice process as soon as a good or content is found that sufficiently satisfies their need (although it may not be the ultimately optimal good), thus, following a concept of "satisficing."[4] How much cognitive resources users spend on a search and choice process depends on how important the respective good is for them: while routine consumption involves comparatively few cognitive resources and a satisficing level is quickly achieved, extraordinary consumption involves more thorough search and more careful choice decisions.[5]

Many online services individualize the ranking of search results and recommendations so that each user receives her individual ranking, based upon (i) personalized data about

2 This article draws particularly on Budzinski, O., Gaenssle S. & Lindstädt-Dreusicke, N. (2022), Data (R)Evolution – The Economics of Algorithmic Search & Recommender Services, in: Baumann, S. (ed.), Handbook on Digital Business Ecosystems (Edward Elgar), pp. 349-366 and Budzinski O., Karg, M. (2023), Gatekeeper, Marktmacht und die Regulierung von Onlinediensten, Staatswissenschaftliches Forum, 6 (1), forthcoming, which deliver more in-depth analyses of the issues discussed here.

3 *Inter alia,* Pan, B., et al. (2007), In Google We Trust: Users' Decisions on Rank, Position and Relevancy, Journal of Computer-Mediated Communication, 12 (3), pp. 801-823.

4 Simon, H. A. (1955), A Behavioral Model of Rational Choice, The Quarterly Journal of Economics, 69 (1), pp. 99-118; Güth, W. (2010), Satisficing and (Un)Bounded Rationality: A Formal Definition and Its Experimental Validity, Journal of Economic Behavior and Organization, 73 (3), pp. 308-316; Caplin, A., Dean, M. & Martin, D. (2011), Search and Satisficing, American Economic Review, 101 (7), pp. 2899-2922; Güth, W., Levati, M. V. & Ploner, M. (2012), Satisficing and Prior-free Optimality in Price Competition, Economic Inquiry, 50 (2), pp. 470-483.

5 Vanberg, V. J. (1994), Rules and Choice in Economics (Routledge); Budzinski, O. (2003), Cognitive Rules, Institutions and Competition, Constitutional Political Economy, 14 (3), pp. 215-235. Examples for routine consumption would be for many consumers the choice of washing powder in the supermarket, music for easy listening, or videos to calm down from a hard day's night. By contrast, more cognitive resources may be invested to the planning of a special holiday trip or media content for a special evening. Individuals differ a lot here, of course.

the user,[6] (ii) data about users that are to some degree similar, and (iii) general knowledge about popular contents. In other words, the underlying algorithms try to estimate the preferences of the individual user based upon the available data and provide a best-match ranking. The quality of the personalized ranking depends on data availability and algorithm intelligence. Generally, the systems work considerably better for mainstream preferences and for homogeneous niche interests than for diversity-preferring non-mainstream interests.

B. Welfare Effects

Economic research identifies three positive welfare effects of individualized ASRS:

- They provide a necessary pre-selection in the face of information overload and, thus, are a necessary condition for consumer choice.
- They provide rankings that approximate the preferences of the users, thus, contributing to a preference-oriented supply in the digital world.[7]
- Due to the individualization, they deliver a broader choice menu to the overall group of users since every user gets a different set of pre-selected items. Thus, an overall larger set of goods is brought to the attention of the users as a whole.

Alternative regimes struggle to provide these welfare effects. A random ranking fails to achieve the first two advantages.[8] A ranking decision by a human editorial board – apart from efficiency considerations – that provides a one-size-fits-all ranking like in the traditional media world of newspapers, magazines, radio, and television channels performs worse in the second and in the third welfare advantage, i.e. the outcome would represent a worse fit to user preferences and the range of pre-selected contents would be smaller.

Notwithstanding their beneficial effects, ASRS still present a barrier to market entry: only those items that get listed/ranked sufficiently prominent de facto participate in market competition. This generates gatekeeping power (already way below any accompanying market power), which can be (ab-)used:

- Self-preferencing comprises strategies where the ranking is employed to systematically up-rank the company's own items and/or to systematically down-rank the items of competitors.[9]
- Media bias refers to the deliberate ideological biasing of ranking results regarding news items and/or cultural agendas.

Alternative regimes struggle to provide these welfare effects. A random ranking fails to achieve the first two advantages

These abusive strategies require a deliberate twisting of the algorithm to implement the ranking bias. The counter-effect, limiting gatekeeping power, would be users switching to competing services if they face artificial distortions of search and recommendation rankings. However, next to having an alternative, this requires that users realize gradual distortions of such rankings. This is unlikely because of the very logic of the usefulness of ASRS: due to systemic information overload, users cannot overview all potential offers and depend on selecting within the pre-selected commodities, services, and contents. Only a recurrent comparison of different services and their rankings could help identifying a gradual decrease in ranking quality due to artificial biasing. This, however, increases transaction costs and, thus, is rationally unlikely to be conducted in routine consumption situations (but may work for extraordinary consumption). Therefore, transparency requirements must be expected to be ineffective (in the majority case of routine consumption) if it is accompanied by increasing transaction costs.

Furthermore, the focus on the preferences of the users may lead to an issue that, by contrast, does not require any deliberate twisting of the algorithm:

> Echo chamber effects and filter bubbles may be the result of the self-reinforcing character if ASRS provide users always with more of the same since these are their estimated prefer-

6 Personalized data usually consists of standard identification data, behavioral data like revealed preferences (for instance, through online shopping and individual search/browsing histories) and stated preferences (like ratings, likes, follows, comments, etc.), and derived data combining the former categories complemented with data of similar individuals (Budzinski, O., Kuchinke, B. A. (2020), Industrial Organization of Media Markets and Competition Policy, in: Rimscha (ed.), Management and Economics of Communication (DeGruyter), pp 21-45).

7 For empirical evidence see, inter alia, Thurman, N., et al (2019), My Friends, Editors, Algorithms, and I, Digital Journalism, 7 (4), pp. 447-469.

8 Evidence can easily be produced by self-experimenting: try to only use page 50 or 100 of the search items for every search inquiry. For many inquiries, no useful hit will be found.

9 With further references see, for instance, Bougette, P., Budzinski, O. & Marty, F. (2022), Self-Preferencing and Competitive Damages: A Focus on Exploitative Abuses, The Antitrust Bulletin, 67 (2), pp. 190-207.

ences. The confrontation with new (types of) content – which may be either just disliked by an individual user or develop taste-building effects (i.e., detecting new things you like) – may not happen anymore. The frequency and amount of such effects – beyond the deliberate ignorance of a specific type of user actively pursuing the entrance into an echo chamber – is controversially discussed in the literature.[10]

03

THE REGULATION OF RECOMMENDATION RANKINGS IN THE DIGITAL SERVICES ACT

A. The Digital Services Act ("DSA")

After a long drafting and negotiation process, the DSA was published in the Official Journal of the European Union on 27 October 2022.[11] It aims to better protect consumers and their fundamental rights online by establishing a transparency and accountability framework for online services. In addition to requirements for the moderation of user-generated content, it also addresses information distortions caused by ASRS by imposing transparency obligations.
The DSA applies to "intermediary services" offered to users that are located or have their place of establishment in the Union (Art. 2 (1) DSA). The due diligence obligations are adapted to the type, size, and nature of the intermediary service and increase gradually in four stages.[12] While only basic obligations apply to infrastructure providers such as internet access providers or domain name registrars, they expand for "hosting service providers" that provide cloud and web hosting services, and "online platforms" that bring sellers and consumers together, which include app stores or online marketplaces. For "very large online platforms" and "very large online search engines" with 45 million monthly active users in the EU (Art. 33 DSA), the DSA establishes the most stringent requirements, as they may pose particular risks for the distribution of illegal content and, thus, may cause societal harms.

B. Recommender Systems in the DSA

The DSA acknowledges that recommender systems have a significant impact on the ability of users to retrieve and interact with information online. It responds to the negative societal effects of ASRS with transparency requirements and obliges services to ensure that users are adequately informed about how recommendation systems affect the display of information. To achieve this, the functionality of a recommendation ranking as well as its parameters shall be explained in an easily comprehensible manner.[13]

Firstly, all providers of online platforms that use recommender systems shall set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommendation rankings, which includes at least the criteria which are most significant in determining the information suggested to the user, as well as the relative importance of those parameters (Art. 27 (1) and (2) DSA).

If several parameters may determine the relative order of information presented to users, providers of online services must make available a functionality that allows users to select and modify at any time their preferred option (Art. 27 (3) DSA). Very large online platforms and very large online search engines will be further obliged to offer users at least one option of the recommendation system which is not based on user preferences and personalized data (profiling) (Art. 38 DSA).

The impact of ASRS must also be explicitly included in the mandatory annual assessment of systemic risks by very large online platforms and very large online search engines (Art. 34 (2) (a) DSA). Besides the risk assessment, those providers also need to take measures to mitigate the systemic risks of their services. For this purpose, the testing and adaption of their ASRS is mandatory (Art. 35 (1) (d) DSA). Pursuant to Art. 40 (1) DSA and upon request, very large online platforms and very large search engines are required to grant access to data that is necessary to assess and monitor compliance with the DSA to the supervision

10 See Gentzkow, M. A., Shapiro, J. M. (2011), Ideological Segregation Online and Offline, Quarterly Journal of Economics, 126 (4), pp.1799-1839; Zollo, F., et al (2015), Debunking in a World of Tribes, in: *arXiv*:1510:04267; Schnellenbach, J. (2018), On the Behavioral Political Economy of Regulating Fake News, ORDO, 68 (1), pp. 159-178.

11 Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1 .

12 DSA, Recital 41.

13 DSA, Recital 70.

and enforcement authorities (Art. 49 (2) DSA).[14] Also upon request, they must explain the design, logic, functioning, and testing of their ASRS (Art. 40 (3) DSA).The authorities can also order that data access is to be given to "vetted researchers" for the detection, identification, and understanding of systemic risks caused by very large online platforms or very large search engines (Art. 34 (1) DSA) and the assessment of the adequacy, efficiency, and impacts of the risk mitigation measures pursuant to Art. 35 DSA (Art. 40 (4) DSA). "Vetted researchers" are subject to various conditions (Art. 40 (8) DSA), which include a university affiliation, their independence of commercial interests, and their capability to fulfill data security and confidentiality requirements.

> ***The DSA acknowledges that recommender systems have a significant impact on the ability of users to retrieve and interact with information online***

C. Transparency as a Regulatory Solution?

The transparency provisions for ASRS in the DSA envisage to promote user autonomy and enable informed choices by reducing information asymmetries between online service providers and users. They affect all online platforms that use algorithmic systems, with very large online platforms again being subject to more extensive obligations. In the light of their market dominance a size-based regulation concept is generally viewed to be appropriate.[15]

The DSA does not attempt to regulate (the diversity or pluralism of) recommendation ranking outputs but aims to empower users to make better-informed choices based on more information on how the algorithms process information. This stands in line with the inherent pro-diversity effect of individualized rankings and the mixed research results concerning echo chamber and filter bubble effects, which do not indicate the necessity of imposing diversity obligations on ASRS outputs (see section 2).

Instead, the DSA focuses on imposing transparency obligations. This is not done by any obligations to disclose algorithms, which (i) are trade secrets, (ii) would restrict competition for the best systems, and (iii) would not effectively help consumers due to the complexity of the matter. It is utopian to reach a level of algorithmic transparency, where it is possible for users to fully understand the logic of an algorithm – which often not even experts do. Thus, the question is whether the limited transparency provisions (as described in section 3.2) will actually empower users to better understand recommender rankings and/or detect artificial biasing. Instead, the transparency obligations may either turn out to be a paper tiger or a transaction costs-increasing tool that most users find annoying.[16]

The DSA obligations focus on disclosing the main parameters that determine the ranking results. On the one hand, this may be too narrow to effectively reduce information asymmetries and enable better-informed choices – or even a detection of biasing. The interdependence of user behavior (uploading, subscribing, consuming, (dis-)liking content, etc.) and the algorithmic output – which mutually influence each other – may not be captured by merely disclosing the main parameters of the algorithms.[17] On the other hand, the willingness of rational users to spend cognitive resources on information and customizing of ASRS are likely to be exhausted very quickly – at least for everyday routine consumption choices (see section 2).

Moreover, even if users get an insight into how recommender rankings work, this does not necessarily increase the probability that they switch to another service. While this is obvious in cases of market dominance of service providers (locking-in consumers),[18] gatekeeping-effects also occur outside the scope of traditional market dominance in less concentrated markets (see section 2). The regulatory goal of informed and autonomous user choices neglects the inherent information overload issues that make individual users dependent on a pre-selection service and give them little power to identify (gradually) suboptimal ranking results. Even if they dislike the way a recommendation ranking works, switching costs may be considerable. The concept of user autonomy based on transparency further bur-

14 These are the European Commission as well as in each member state the Digital Services Coordinator of establishment.

15 Leerssen, P. (2020), The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems, European Journal of Law and Technology, 11 (2), p. 47.

16 Do the ubiquitous cookie setting pop ups in Europe really improve online activities?

17 Rieder, B., Matamoros-Fernández, A. & Coromina, Ó. (2018), From ranking algorithms to 'ranking cultures': Investigating the modulation of visibility in YouTube search results, Convergence, 24 (1), pp. 50-68, Leerssen, P. (2022), Algorithm Centrism in the DSA's Regulation of Recommender Systems, VerfBlog, 2022/3/29, DOI: 10.17176/20220330-011148-0.

18 Leerssen, P. (2020), The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems, European Journal of Law and Technology, 11 (2), p. 25.

dens individuals with additional transaction costs: they are expected to seek and interpret information by themselves.[19] The higher the information costs of users, the greater the leeway tends to be for service providers.[20] Ironically, forcing users to recognize and deal with settings (e.g. by pop-ups preventing an uninformed use) also increases transaction costs, especially regarding routine consumption, and may be welfare-decreasing in this regard (see section 2).

Furthermore, in scenarios with personalized recommendation rankings, the disclosure of the main algorithm-parameters offers no insight to possible systemic biases in the algorithm output, since the ranking is different for each user.[21] In the past, researchers have tried to conduct studies surveying a large number of different user-outputs, but platform-providers have put in a lot of effort to prevent researchers to evaluate a larger base of algorithmic outputs across society.[22] At this point, the DSA provides an improvement: Data access for vetted researchers pursuant to Art. 40 (4) for systemic risk management and mitigation includes ASRS (Art. 34 (2) (a) and Art. 35 (1) (d)).

In addition to the disclosure of the main parameters that influence a recommender ranking, very large online platforms and very large search engines must offer an option of their ASRS that is not based on user preferences (Art. 38 DSA), which ultimately increases consumer choice on the system level.[23] While it is up to the individual service provider to pick an alternative (see section 2 for possible alternatives and their welfare effects), the most probable solution, is an algorithm-based display of the most popular content, which leads to the same content being displayed to every user who choses this option. An editorial selection looks unlikely since this is precisely what the platform providers do not claim to be, and random rankings would be accompanied by a considerable loss of quality in the search and recommender ranking service – up to the point of the search system being completely useless. From an economic point of view, an obligation to a non-personalized ranking option can lead to a reduction in the diversity of algorithm outputs (see section 2), which would be an undesirable regulatory side effect.

Depending on the design and implementation, users could be annoyed by a mandatory selection decision when forced to visit a website for a personalized/non-personalized ranking system (annoyance costs as a type of transaction costs). Such a design would not be economically beneficial as it would increase users' transaction costs. Furthermore, the parameters that users can ultimately influence are only a fraction of what the algorithm processes, which could create a misleading image of transparency for users.[24] Overall, it may therefore be doubtful whether Art. 38 DSA will bring a desirable development regarding the comprehension of ASRS in addition to merely increasing consumers' freedom of choice on the system level by the additional non-personalized option. Notwithstanding, an intelligent design of this additional option might benefit some consumers while not decreasing welfare for the majority of routine consumption decisions – and thus do no harm.

04
CONCLUSIONS

Regulating ASRS provides a challenge of balancing beneficial effects with possible pitfalls and scope for abuse. The DSA provides a cautious regulatory approach that may not achieve a lot of effects from an economic perspective of rational choice but – depending on the design and implementation of the mandatory non-personalized option – is likely to leave the beneficial effects untouched. Still, understanding the behavior of users in choice situations (as outlined in section 2) is paramount to further develop any regulation of ASRS. Based upon our welfare analysis in section 2, we can

19 Edwards, L., Veale, M. (2017), Slave to the Algorithm? Why a 'Right to Explanation' is probably not the remedy you are looking for, Duke *L*aw *&* *T*echnology *R*eview, 16 (1), pp. 18-84 (67); Ananny, M., Crawford, K. (2018), Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability, new media & society, 20 (3), pp. 973-989 (979).

20 Schweitzer, H., et al (2018), Report for the Federal Ministry for Economic Affairs and Energy (Germany), n. 220; see also Scott-Morton, F., et al (2019), Report of the Committee for the Study of Digital Platforms – Market Structure and Antitrust Subcommittee, pp. 35-38.

21 Leerssen, P. (2022), Algorithm Centrism in the DSA's Regulation of Recommender Systems, VerfBlog, 2022/3/29, DOI: 10.17176/20220330-011148-0.

22 Heldt, A., Kettemann, M. C. & Leerssen, P. (2020), The Sorrows of Scraping for Science: Why Platforms Struggle with Ensuring Data Access for Academics, VerfBlog, 2020/11/30, DOI:10.17176/20201130-220222-0.

23 Helberger, N., et al (2021), Regulation of news recommenders in the Digital Services Act: empowering David against the Very Large Online Goliath, Internet Policy Review, accessible at: https://policyreview.info/articles/news/regulation-news-recommenders-digital-services-act-empowering-david-against-very-large.

24 Helberger, N., et al (2021), Regulation of news recommenders in the Digital Services Act: empowering David against the Very Large Online Goliath, Internet Policy Review, accessible at: https://policyreview.info/articles/news/regulation-news-recommenders-digital-services-act-empowering-david-against-very-large.

summarize whether and how the DSA combats the downsides of ASRS:

- **Does the DSA solve the problem of self-preferencing?** The answer is a clear no. However, self-preferencing is explicitly addressed by his sister act, the Digital Markets Act, which prohibits self-preferencing in general. Unfortunately, the DMA obligation only applies to selected so-called core platform services and will not address many ASRS with gatekeeping effects.[25] The DSA would have been an option to extend the ban of self-preferencing beyond core platform services.

- **Does the DSA solve the problem of (ideological) media bias?** Pure transparency obligations are probably too weak for this problem. For news and news-related rankings, an obligation to consider the quality of a source within the ASRS may be a way forward despite the non-trivial issue of defining the right quality criteria.[26]

- **Does the DSA solve the problem of echo chambers/filter bubbles?** This cannot be expected as well but maybe they are not the most pressing problem, especially if the former issue is addressed.

> *Regulating ASRS provides a challenge of balancing beneficial effects with possible pitfalls and scope for abuse*

25 See on the DMA and gatekeeping power: Budzinski, O., Mendelsohn, J. (2022), Regulating Big Tech: From Competition Policy to Sector Regulation? (Updated October 2022 with the Final DMA), http://dx.doi.org/10.2139/ssrn.4248116.

26 See also Möller, J., et al (2018), Do not blame it on the algorithm: an empirical assessment of multiple recommender systems and their impact on content diversity, Information, Communication & Society, 21 (7), 959-977; Helberger, N. (2019), On the Democratic Role of News Recommenders, Digital Journalism, 7 (8), 993-1012.

WHAT'S **NEXT**

For January 2023, we will feature a TechREG Chronicle focused on issues related to Web3.

ANNOUNCEMENTS

CPI TechREG CHRONICLES February 2023

For February 2023, we will feature a TechREG Chronicle focused on issues related to **Machine Learning**.

Contributions to the TechREG Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI TechREG Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden (ssadden@competitionpolicyinternational.com) with the subject line "TechREG Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers in any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

ABOUT US

Since 2006, **Competition Policy International** ("CPI") has provided comprehensive resources and continuing education for the global antitrust and competition policy community. Created and managed by leaders in the competition policy community, CPI and CPI TV deliver timely commentary and analysis on antitrust and global competition policy matters through a variety of events, media, and applications.

As of October 2021, CPI forms part of **What's Next Media & Analytics Company** and has teamed up with **PYMNTS**, a global leader for data, news, and insights on innovation in payments and the platforms powering the connected economy.

This partnership will reinforce both CPI's and PYMNTS' coverage of technology regulation, as jurisdictions worldwide tackle the regulation of digital businesses across the connected economy, including questions pertaining to BigTech, FinTech, crypto, healthcare, social media, AI, privacy, and more.

Our partnership is timely. The antitrust world is evolving, and new, specific rules are being developed to regulate the so-called "digital economy." A new wave of regulation will increasingly displace traditional antitrust laws insofar as they apply to certain classes of businesses, including payments, online commerce, and the management of social media and search.

This insight is reflected in the launch of the **TechREG** Chronicle, which brings all these aspects together — combining the strengths and expertise of both CPI and PYMNTS.

Continue reading CPI as we expand the scope of analysis and discussions beyond antitrust-related issues to include Tech Reg news and information, and we are excited for you, our readers, to join us on this journey.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL