Responses to the European Commission's consultation on the Digital Services Act (DSA)

September 2020

For questions and comments, please contact the authors:
Aline Blankertz (ablankertz@stiftung-nv.de)
Dr. Julian Jaursch (jjaursch@stiftung-nv.de)

Stiftung Neue Verantwortung (SNV) is a Berlin-based, non-profit think tank working on current political and societal challenges posed by new technologies. Not only do we invite government officials but everyone seeking information to engage with our work whether through giving us feedback on publications, participating in our events or seeking direct advice. Our experts work independently from partisan interests or political affiliations.

Learn more at https://stiftung-nv.de.

0. Summary of key points

We welcome the European Commission's plans to update the rules for digital services by proposing a Digital Services Act (DSA). An EU-wide legal framework is vital for a digital market that can function well across countries in order to safeguard citizens' fundamental rights, and to provide the necessary scale for European competition and innovation. Since the E-Commerce Directive was passed, internet usage and online business models have changed considerably, and new, wide-ranging benefits as well as harms associated with the digital sphere have become apparent.

Gatekeeper platforms have produced significant benefits by lowering the barriers to enter the markets that they serve compared to the harder-to-search non-platform or even offline markets. These benefits should be preserved as much as possible, alongside positive externalities such as network effects.

However, gatekeeper platforms can also disengage consumers from making deliberative choices, which is harmful for consumer welfare, markets and, in some instances, democratic processes. It is highly problematic if consumers face barriers to see and consider options that a gatekeeper platform does not promote, and are instead made to believe they get a full and supposedly objective picture of "the market". The widespread activities of the owners of gatekeeper platforms on downstream or related markets mean that gatekeepers have an incentive not to provide the best outcome for the consumer (i.e., showing them the product or content that best fits consumers' needs), but those outcomes favoring the gatekeepers' own commercial interests. This has a strong potential to harm competition on those related markets and to make the gatekeepers' position even less contestable. Furthermore, some gatekeeper platforms, especially social media and video portals offering algorithmic information and media spaces for citizens, have amplified risks for fair political and social debates. Disinformation and discriminatory content can spread both widely and in a targeted manner in such online information spaces. This poses the danger of undermining democratic processes, as citizens find it harder to access trustworthy information and participate in democratic debates.

We appreciate the opportunity to participate in the Commission's consultation on the DSA. In this summary, we highlight some of our key responses to the consultation. First, we provide considerations that should form part of the potential regulatory framework for gatekeeper platforms. Second, we emphasize that dealing with disinformation requires establishing procedural accountability. Third, we describe how online advertising should be made more transparent not just for advertisers, but also for authorities, civil society organizations and consumers.

Creating an EU regulatory framework for gatekeeper platforms

Ex-ante regulation for gatekeeper platforms is sensible to reduce potential adverse effects on the economy and the society. Various expert reports have confirmed that while traditional competition policy has its merits, its limitations in digital markets include lengthy procedures (during which competitive harm becomes increasingly irreversible) and the requirement of culpability. Regulation has the benefit of setting the rules ex ante such that procedures to ensure adherence to regulation can be shorter and such that firms do not have to be found guilty of anti-competitive conduct before certain rules can be applied to them. The Furman Report to the UK government provides helpful advice on how to set up such a regulation.

There are two types of obligations we consider particularly helpful that should be considered for inclusion on a list of special obligations for gatekeeper platforms:

First, the DSA should require gatekeeper platforms to provide meaningful transparency and data on their internal workings to authorities, researchers, and, where appropriate, the public. Their important role to the economy and democracy necessitates comprehensive transparency standards that enable society to understand the impact of gatekeeper platforms on markets as well as on political and social debates. For example, gatekeeper platforms should report on their algorithmic recommender systems, and their content moderation policies and practices. The platforms' interest in keeping business-sensitive information private needs to be balanced with the significant public interest in understanding their impact. Transparency is also a prerequisite for assessing the platforms' compliance with EU and international human rights law.

Second, the DSA should mandate gatekeeper platforms to provide both their business and their personal users with data portability, the scope of which needs to go far beyond that stipulated in the EU's General Data Protection Regulation (GDPR). Data portability should be continuous, include a broad range of user-specific data, and users should be able to move data directly between platforms. Enabling users to port their data between services is important to reduce data-related lock-in like in app store ratings or location history. While more portability may be desirable for platforms without the gatekeeper status in certain markets, lock-in is a greater concern for gatekeeper platforms and they are more likely to have the relevant technical expertise to implement it.

There are two types of gatekeeper platform behavior we consider particularly harmful that should be considered for inclusion on a deny list:

First, the DSA should introduce higher hurdles for gatekeeper platforms with a conglomerate structure to merge data sets including personal data and for using personal data across services. The GDPR does not explicitly address the special dynamics associated with data-dominant firms. However, in dealing with these firms, users are deprived of any meaningful choice. Hence, gatekeeper platforms should be prevented from engaging in excessive data merging across services. The German Federal Court of Justice recently published its detailed judgment in the case Bundeskartellamt v. Facebook which is instructive on the understanding of choice as an objective of competition policy.

Second, the DSA should establish clearer rules for gatekeeper platforms regarding how to treat their own services. Harm can arise especially if a gatekeeper platform gives preferential treatment to its own services if this is not based on criteria that benefit consumers. In the digital world, it is often difficult to distinguish between vertical and horizontal relationships between services because this may depend on the user group (for example, some may use Google as an entry point for product search and continue to Amazon, while others may start at Amazon directly). Hence, clear criteria need to be developed to distinguish when preferential treatment is problematic. More evidence is necessary to specify when and what kind of prohibition is useful to balance the harm to competition and the scope for companies to exploit synergies among their services.

A regulatory horizontal framework is compatible with and should be complemented with a market-specific approach to address structural concerns that persist despite regulation. The New Competition Tool (NCT) would be a suitable addition to ex-ante regulation. With a well-designed NCT – including a broad set of remedies available, appropriate checks and

balances, and no need for establishing culpability – ex-ante regulation can focus on the most problematic types of behavior across markets.

Tackling the spread of disinformation online

The need for EU-wide regulation is particularly evident with regard to information gatekeepers such as social media companies, search engines and video apps. They provide digital communication and media spaces, where citizens debate and form their opinions on social and political topics. While platforms can assist such democratic processes, serious dangers for democracy arise as well: Disinformation and discriminatory content spread online can considerably infringe upon citizens' basic human right to form their political opinions without interference, and can furthermore negatively affect individual and public health, as is visible in the COVID-19 pandemic.

Continuing to rely only on national (criminal law) rules to tackle these challenges is misguided and not sufficient. Such rules largely focus on removing individual pieces of harmful/illegal content without addressing the overarching market failures that create the incentives to not tackle disinformation more effectively. Besides, neither governments nor companies should be left on their own to decide what content to delete, and thus to decide how to balance free speech concerns with potential harms stemming from disinformation and discrimination.

The DSA should provide clear legal guidance for platforms, that does not focus on enforcing decisions on individual pieces of content, but instead focuses on the processes for accountable corporate decision-making. This could include a common EU framework for content moderation policies and practices, based on international human rights standards, mandatory transparency and accountability reporting as well as independent oversight.

Establishing binding rules and oversight for online advertising

Most behavioral data should not be collected in the first place because its economic value is not proportionate to the harm it creates. The deep intrusion into privacy is not offset by the little added value created mainly for advertisers, most of which is extracted by the data-collecting platform. The current terms and conditions do not give individuals an effective way to opt out of those practices.

However, even where using certain behavioral data is in the interest of users and society, big ad-tech platforms do not provide users, researchers and regulators easy-to-access and easy-to-understand insights into how personal behavioral data is being used to target and deliver advertising. This is detrimental to consumer welfare, as users are left in the dark as to who is paying to reach them and how, even though their personal behavior data is being exploited for the ad targeting and delivery.

The DSA should include the following measures aimed at platforms that would establish more meaningful transparency for online advertising:

- Mandatory, expanded and vastly improved ad archives including information on targeting and engagement metrics, data sources, and ad financing
- Mandatory, expanded transparency reporting on processes for ad targeting and ad delivery
- Mandatory, improved ad disclaimers
- Mandatory advertiser verification

Compliance with these requirements should be checked by an independent oversight body that has the technical expertise as well as staff and budget resources to audit transparency reports.

Transparency, accountability and oversight mechanisms are especially crucial for online *political* advertising. When advertising, candidates, political parties and other campaigners are not trying to sell products and services, but pay to shape political debates and influence voting decisions. A lack of options for public interest scrutiny of online political ads can therefore weaken the legitimacy and integrity of elections and political campaigning more generally. In addition to the transparency standards mentioned above, further rules for political advertising should be established, including restrictions on behavioral microtargeting and expanded financial accountability reporting by platforms and political advertisers such as European parties and candidates. In sync with other Commission initiatives, especially the European Democracy Action Plan, the DSA should define the baseline requirements for transparency and accountability for paid online political messaging in Europe.

We thank the Commission for providing the opportunity to submit our responses to the consultation and look forward to engaging further on this important legislative proposal in the future, not only with the Commission and the European Parliament but all interested stakeholders.

Stiftung Neue Verantwortung

I. How to effectively keep users safer online?

Main issues and experiences B

19 What good practices can you point to in handling the dissemination of illegal content online since the start of the COVID-19 outbreak?
Platforms have taken a number of steps that they were reluctant to implement just a few years ago, including information panels with authoritative sources, fact-checking, ad credits for scientific organizations, downranking demonstrably false content and alerting users to disinformation. These steps should be built upon to tackle disinformation in other fields apart from (public) health such as climate change and elections. Crucially, there should be standards as to what platforms can do, what transparency is required for their actions and how consistent enforcement can be ensured. While for an issue such as COVID-19, swift action and government-platform coordination was necessary and helpful, in other cases, it can be problematic if platforms and/or governments decide what content is being demoted and what is deemed an "authoritative source" without independent oversight.

Generally, it should be noted that good practices against disinformation and illegal content must be a combination of regulation (on this, see the answers in part III) and education. Empowering citizens of all ages to develop and enhance their digital news literacy is vital in dealing with disinformation online, be it on COVID-19 or other topics.

21 Do you consider these measures appropriate?
No

22 Please explain.
The measures described in the response to question 19 are laudable and helpful, but not enough for two primary reasons: First, they are uncoordinated, voluntary, ad-hoc, short-term measures. It would be better if the platform response to e.g. COVID-19 disinformation were following standardized guidelines (see answer to question 19) and were legitimized by lawmakers. Second, while all of the measures such as fact-checking or pointing users to reliable sources are a great way of alleviating some of the obvious symptoms of COVID-19 disinformation, they do not address the underlying issues plaguing platforms. These include the mass tracking of personal behavioral data to optimize algorithms that can lead people to COVID-19 disinformation, the lack of regulatory oversight and the weak enforcement of data protection rules. These issues are addressed in other parts of this consultation and will thus not be elaborated on here.

Main issues and experiences C

2 To what extent do you agree with the following statements related to online disinformation?

	Fully agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Fully disagree	I don't know/No reply
Online platforms can easily be manipulated by foreign governments or other coordinated groups to spread divisive messages	X					
To protect freedom of expression online, diverse voices should be heard		X				

Disinformation is spread by manipulating algorithmic processes on online platforms		X				
Online platforms can be trusted that their internal practices sufficiently guarantee democratic integrity, pluralism, nondiscrimination, tolerance, justice, solidarity and gender equality.					X	

3 Please explain.
Online platforms are not the cause of disinformation, which is a phenomenon predating digital platforms. Yet, platforms are one of the major amplifying vectors contributing to a new quantity and quality of disinformation (see especially pages 7-11 in https://www.stiftung-nv.de/sites/default/files/regulatory_reactions_to_disinformation_in_germany_and_the_eu.pdf). The digital news and information spaces that platforms provide are vast, often global in reach and thrive because large, centralized platforms use algorithms to keep people engaged on their platforms, based on massive amounts of personal behavioral data.

On the third line in the table above, two things are important to point out:
First, "manipulating algorithmic processes" is not only done by foreign governmental actors. Rather, disinformation is spread from domestic, non-state actors as well (see https://www.stiftung-nv.de/sites/default/files/snv_fakten_statt_fakes.pdf). This understanding is key to tackling disinformation, as otherwise the view is too narrowly focused on foreign governmental spreaders of disinformation. Second, "manipulating algorithmic processes" is not the only, and possibly not the most important way, that disinformation spreads. Actors, whether foreign or domestic, do not necessarily "break" or "abuse" the algorithm. Algorithmic processes can also merely be used as intended to spread disinformation: Content moderation algorithms are set to maximize user engagement on the platform, e.g. measured in likes, clicks, shares, comments and views, and this type of content tends to be divisive, polarizing and radical content, including disinformation. A study has highlighted that content which stokes the feelings "anger" and/or "fear" tend to work best in some algorithmic settings (see https://journals.sagepub.com/doi/full/10.1177/2056305119829859).

On the last line in the table above: Voluntary, self-regulatory measures by platforms, even those coming after necessary and welcome pressure from the Commission, have not been sufficient at all. Most large platforms such as Facebook/Instagram, Google/YouTube, Twitter and TikTok cannot be trusted with and should not be left alone with fulfilling the mentioned responsibilities. While some large platforms have taken steps to tackle disinformation, these efforts have been rudimentary, uncoordinated and cannot be enforced by legislators or regulators, as they are non-binding. Despite their efforts, platforms have, time and again, failed to stem the spread of disinformation on their services. Examples of this do not only concern disinformation on elections, but also on public health issues such as the COVID-19 pandemic, societal issues such as migration and climate change as well as overarching conspiracy myths about political and media leaders. Platforms lack strong incentives to tackle disinformation, as some of the most engaging content is often disinformation, as it stokes anger and fear (see paragraph above).

4 In your personal experience, how has the spread of harmful (but not illegal) activities online changed since the outbreak of the COVID-19 pandemic? Please explain.
Disinformation on COVID-19 included supposed "miracle cures", lies about who supposedly created the virus and falsehoods about how it is spread. Often, these narratives were connected to existing disinformation narratives such as anti-migrant, anti-elite, anti-tech or antisemitic tropes. There is not much change in how COVID-19 disinformation spreads, but the challenges of disinformation in general are heightened because it is a topic of immediate, global concern for public health.

5 What good practices can you point to in handling such harmful activities since the start of the COVID-19 outbreak?
Please see answer to question 19 in part I, B. Please also note that we advise against trying to broadly distinguish between "harmful" and "illegal" content/activities. While such a distinction might be possible in some cases, in most circumstances, the line between harmful, but legal, and illegal content is blurred. Regulation should thus not primarily focus on how individual pieces of content are dealt with but establish transparency and accountability guidelines (see answers in part III).

Clarifying responsibilities for online platforms and other digital services

1 What responsibilities should be legally required from online platforms and under what conditions? Should such measures be taken, in your view, by all online platforms, or only by specific ones (e.g. depending on their size, capability, extent of risks of exposure to illegal activities conducted by their users)? If you consider that some measures should only be taken by large online platforms, please identify which would these measures be.

	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)	Yes, only by larger online platforms	Yes, only platforms at particular risk of exposure to illegal activities by their users	Such measures should not be required by law
Maintain an effective 'notice and action' system for reporting illegal goods or content	X			
Maintain a system for assessing the risk of exposure to illegal goods or content	X			
Have content moderation teams, appropriately trained and resourced	X			
Systematically respond to requests from law enforcement authorities	X			
Cooperate with national authorities and law enforcement, in	X			

accordance with clear procedures				
Cooperate with trusted organisations with proven expertise that can report illegal activities for fast analysis ('trusted flaggers')	X			
Detect illegal content, goods or services				X
In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law	X			
Request professional users to identify themselves clearly ('know your customer' policy)	X			
Provide technical means allowing professional users to comply with their obligations (e.g. enable them to publish on the platform the pre-contractual information consumers need to receive in accordance with applicable consumer law)	X			
Inform consumers when they become aware of product recalls or sales of illegal goods	X			
Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities	X			
Be transparent about their content policies, measures and their effects	X			
Maintain an effective 'counter-notice' system for users whose goods	X			

or content is removed to dispute erroneous decisions				
Other. Please specify				

2 Please elaborate, if you wish to further explain your choices.
This answer pertains to illegal content on media intermediaries (and less to illegal goods). We distinguish between spreading illegal content and illegal goods online. While both issues can cause harm and both, in some ways, make use of platforms' non-transparent algorithmic information spaces or marketplaces, there are important differences. These concern, among other things, the types of platforms used, the intentions behind the spread of illegal goods/content and the societal as well as democratic aspect of the two issues. The latter point is especially crucial in our view, as the spread of illegal content arguably concerns more people, albeit indirectly, and concern democratic processes such as political opinion formation and elections, which is not always given with illegal goods. This is not at all to diminish the individual and social dangers of illegal goods sold online or to say that platforms should not be held accountable for their role in this.

Platforms offering news and information spaces online should be held to binding transparency and accountability mechanisms. This includes reporting obligations and oversight regarding their human rights due diligence, content moderation practices and compliance with privacy rules.

Generally, platforms should adhere to the rules mentioned in the table above. There should be exceptions for non-critical platforms. The criteria for what could be considered non-critical vary depending on what type of platform is addressed. For instance, social media companies don't have to be big to potentially shape and distort political and social debates, and can thus be critical. Simultaneously, large platforms that operate on a business-to-business level might be less critical despite their size. Therefore, when granting exemptions from the above-mentioned obligations, a number of criteria need to be taken into consideration.

Regarding the cooperation with law enforcement (the fifth line in the table above), it is crucial to stress that this should only happen as a last resort and under "clear procedures" that do not undermine human rights such as those to freedom of expression and the right to privacy (including encrypted communication). Law enforcement should always use channels for due process and there should not be no pressure on platforms to provide data outside of clearly defined legal frameworks.

Regarding the detection of illegal goods and content (the seventh line in the table above), it should be clarified that this should not happen solely based on AI systems without human oversight (please see also the answer to question 6 below).

3 What information would be, in your view, necessary and sufficient for users and third parties to send to an online platform in order to notify an illegal activity (sales of illegal goods, offering of services or sharing illegal content) conducted by a user of the service?

Precise location: e.g. URL	X
Precise reason why the activity is considered illegal	X
Description of the activity	X

Identity of the person or organisation sending the notification. Please explain under what conditions such information is necessary:	
Other, please specify	

4 Please explain.
Notifications need to be easily accessible and understandable for users. For instance, descriptions of potentially illegal activities should not be required in precise legal terminology.

6 Where automated tools are used for detection of illegal content, goods or services, what opportunities and risks does their use represent as regards different types of illegal activities and the specificities of the different types of tools?
This response relates mostly to illegal content (not illegal goods).

Due to the large scale of some big online platforms, it can be become necessary to use automated tools to detect illegal content. However, such AI tools carry significant risks, as they are not yet powerful enough to reliably detect illegal speech. Platforms that have invested millions of dollars into their automated tools have said so themselves (https://www.theverge.com/interface/2020/3/18/21183549/coronavirus-content-moderators-facebook-google-twitter). Most crucially, relying only on automated tools to detect supposedly illegal content risks labeling (and potentially) deleting content that is not actually illegal, thereby infringing on citizen's rights to freedom of expression.

No matter what type of automated content moderation is employed – data hash technology, image recognition, metadata filtering, natural language processing (NLP) or a combination of these – automated tools so far fail to have a contextual understanding of human language, i.e. accurately reflecting speakers' nuances of tone, regional/cultural/language differences or differences of online communication across platforms. All of the mentioned tools can be only as good as the dataset that is used to train them, which oftentimes is not good enough to account for the aforementioned nuances of human speech. Moreover, datasets can be biased based on their creators' biases. While automated content moderation might work quite well with some content (e.g. detecting copyrighted material), it is largely unsuitable for detecting hate speech and/or disinformation, as these terms are not and probably cannot be clearly defined across the EU. For an elaboration on these points, see https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/.

Thus, automated tools should be used with caution and their use should not be mandated by law. There should be safeguards in place to ensure human review of potentially illegal content (there needs to be vast improvements as to how content moderators are paid and treated, as this work can lead to serious psychological harm, see https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_content_moderation_report_final_version?fr=sZWZmZjI1NjI1Ng). There should be transparency standards in place for those platforms using (automated) content moderation, which could be stricter for bigger platforms. This should include requirements to report of (automated) content moderation decisions to users, researchers and regulators. For instance, there should be regular reports on the content moderation policies and practices, highlighting the numbers of content takedowns. It should also include a robust notice mechanism for users whose content has been flagged or removed by (automated) content moderation tools. The Santa Clara Principles can inform this debate (santaclaraprinciples.com).

7 How should the spread of illegal goods, services or content across multiple platforms and services be addressed? Are there specific provisions necessary for addressing risks brought by:
a. Digital services established outside of the Union?
b. Sellers established outside of the Union, who reach EU consumers through online platforms?
On a: Digital services established outside of the EU should also fall under the DSA, similarly to how the GDPR is valid for all data-processing entities reaching EU citizens.

9 What should be rights and responsibilities of other entities, such as authorities, or interested third-parties such as civil society organisations or equality bodies in contributing to tackle illegal activities online?
This response relates to illegal content and civil society involvement in tackling its spread. The European Commission should support the creation of an ambitious, decentralized framework fund for civil society, journalists, and researchers across the EU working to tackle disinformation. This would ensure the healthy participation and empowerment of independent organizations to both counter disinformation and hold platforms accountable for upholding democratic principles. This framework should include smaller and more flexible funding than currently available in order to support organizational resilience. In response to recurrent threats and abuse, we would urge that this EU framework additionally provides funding for both the physical and online security of civil society organizations.

A flexible funding scheme like this would also strengthen civil society and academia to serve as an accountability mechanism to ensure that platforms' community standards are being applied successfully. Accountability could be reinforced by EU monitoring of how researchers' and activists' findings lead to action by the companies in a timely manner.

Funding should be invested in supporting independent quality news media and journalism, empowering fact-checkers, disinformation monitoring, investing in media and digital news literacy for all ages, supporting civil society and academic research and public interest actions, but also in encryption tools and censorship-circumventing technologies.

The fund could be financed by a contribution from ad platforms to finance quality journalism and academic as well as civil society research and actions on disinformation and election interference. The fund could also channel funding from other donors, so as to more effectively distribute different sizes of grants to the variety of actors involved. Such a clearing-house mechanism of funding was recommended by the High Level Expert Group on Fake News in their report (page 29 in https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation). The example of the United States' Open Technology Fund could be followed, with its support to an inclusive variety of independent actors working to counter disinformation in its diversity. By creating this body at the EU level, it could overcome some of the dangers of political meddling and problems of independence that the OTF has experienced.

10 What would be, in your view, appropriate and proportionate measures for online platforms to take in relation to activities or content which might cause harm but are not necessarily illegal?
The Commission and national governments should refrain from mandating deleting such content, as definitions are murky, vary across cultures, time, language and political system

and run the danger of "overblocking". If platforms use their own tools and measures to detect and tackle harmful but legal content (which they are and should be free to do), the DSA should mandate that users, researchers and oversight bodies should have full disclosure about these measures. For example, a prescription as described by the NGO European Digital Rights for appropriate, proportionate and transparent measures surrounding potentially harmful content could be envisioned.

There could also be prescriptions in the DSA regarding notifications and enhanced user choice. For instance, notifying users of potential disinformation, for example, by adding labels or links to other sources can be more useful than deletion. Clear, easy-to-access and easy-to-use redress mechanisms should be required (see Santa Clara Principles, https://santaclaraprinciples.com/).

"Downranking" such content would reduce its visibility, but also runs the risk of hiding valid opinions and points. Therefore, if such downranking occurs, it should be made transparent and explained.

In general, activity dealing with individual pieces of content, while important, must be accompanied by structural regulatory efforts such as transparency and accountability measures at the platforms.

12 Please rate the necessity of the following measures for addressing the spread of disinformation online. Please rate from 1 (not at all necessary) to 5 (very necessary) each option below.

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know /No answer
Transparently inform consumers about political advertising and sponsored content, in particular during election periods					X	
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with user complaints					X	
Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives				X		
Transparency tools and secure access to platform data for trusted researchers in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it					X	
Transparency tools and secure access to platform data for authorities in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it			X			

Adapted risk assessments and mitigation strategies undertaken by online platforms					X	
Ensure effective access and visibility of a variety of authentic and professional journalistic sources				X		
Auditing systems for platform actions and risk assessments					X	
Regulatory oversight and auditing competence over platforms' actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on the manipulation and amplification of disinformation					X	
Other (please specify)						

13 Please specify.
On "other" in the table above: Generally, it should be noted that tackling disinformation needs to be a combination of regulation and education. On regulation: Rules from the DSA should not mandate deleting disinformation, as disinformation is ill-defined and not generally illegal. Neither platforms nor governments should be put in the position to determine on their own what constitutes disinformation and what constitutes high-quality information. On education: Empowering citizens of all ages to develop and enhance their digital news literacy is vital in dealing with disinformation online. Support for news literacy and education programs need to be considered alongside regulatory efforts.

14 In special cases, where crises emerge and involve systemic threats to society, such as a health pandemic, and fast-spread of illegal and harmful activities online, what are, in your view, the appropriate cooperation mechanisms between digital services and authorities?
Due to the importance that digital platforms play in many people's information space, there should be standard procedures in place to ensure government-platform cooperation with checks and balances. While in some cases of systemic threats to society, like a natural disaster, it might be relatively easy to identify authoritative sources, in other, more political settings, it is harder. Favoring government sources can be dangerous as well. That is why standard procedures, for example in the form of a checklist, should seek to establish what sources are presented how and under what circumstances to what users. These procedures should be publicly available and subject to regular review, to increase trust of citizens in the information they are receiving in times of crisis.

14 What would be effective measures service providers should take, in your view, for protecting the freedom of expression of their users? Please rate from 1 (not at all necessary) to 5 (very necessary).

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know /No answer
High standards of transparency on their terms of service and removal decisions					X	

Diligence in assessing the content notified to them for removal or blocking					X	
Maintaining an effective complaint and redress mechanism					X	
Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended					X	
High accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts					X	
Enabling third party insight – e.g. by academics – of main content moderation systems					X	
Other (please specify)						X

16 Please explain.
Measures that introduce top-level, industry-wide transparency and accountability standards are to be preferred over measures tackling only speech issues and removing illegal content.
For that reason, the measures mentioned above are equally important. Human oversight is crucial for all of the action points mentioned. Certain standards need to be applied across all platforms, while larger platforms should face more stringent requirements to invest resources in dealing with freedom of expression issues, content moderation and appropriate notice and redress mechanisms.

17 Are there other concerns and mechanisms to address risks to other fundamental rights such as freedom of assembly, non-discrimination, gender equality, freedom to conduct a business, or rights of the child? How could these be addressed?
There are many concerns related to human rights abuses facilitated by the current platform architecture. For example, see the human rights risk scenarios affiliated with targeted advertising here (https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf) and those associated with algorithmic decision-making here (https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf). These risks relate not only to freedom of expression and information (UDHR art. 19), right to life, liberty and security of person (UDHR art. 3), non-discrimination (UDHR art. 7, art.23), freedom of thought (UDHR art. 18), freedom of association (UDHR art. 20), right to take part in the government of one's country, directly or through freely chosen representatives (UDHR art. 21). The papers offer detailed examples and scenarios explaining all of these potential rights violations.

Options to address these issues (beyond the transparency and accountability measures highlighted in answers in part II) are (source: https://rankingdigitalrights.org/governments-policy/):

- Requirement for platforms for human rights due diligence: Companies should be compelled to conduct risk assessments to identify potential human rights impacts and harms that could occur in relation to the use of the company's platform, service, or device. Governments should require companies to carry out credible due

diligence, assessing the impact and risks of their operations and policies on users' freedom of expression and privacy. Companies should also be required to provide meaningful grievance and remedy mechanisms, and to ensure that the law enables meaningful legal recourse and remedy for violations of these rights.

- Requirement for platforms to disclose human rights risks: Disclosures should include risks associated with their business as well as steps companies are taking to mitigate those risks. Specifically, laws should require companies to publish information about potential human rights impacts or harms, including those related to freedom of expression and privacy; implement proactive and comprehensive impact assessments; and establish effective grievance and remedy mechanisms.

18 In your view, what information should online platforms make available in relation to their policy and measures taken with regards to content and goods offered by their users? Please elaborate, with regards to the identification of illegal content and goods, removal, blocking or demotion of content or goods offered, complaints mechanisms and reinstatement, the format and frequency of such information, and who can access the information.
This response relates to disinformation and illegal content.

Studying disinformation is made exceedingly difficult not only by insufficient opportunities for civil society involvement (see response to question 9), but also by a lack of data access from dominant platforms. Data is often much more readily available to advertisers than to academic and civil society researchers and activists tackling disinformation online. GDPR-compliant data access is therefore a necessity to improve the understanding of digital disinformation. Claims by platforms and governments that GDPR-compliant access is not possible are unfunded (see, for example, "A Preliminary Opinion on data protection and scientific research"; "Operationalizing Research Access in Platform Governance What to Learn from Other Industries?"). The European Commission should actively facilitate enhanced access to platform data for public interest scrutiny and research, taking into consideration existing work and proposals by civil society (e.g. https://algorithmwatch.org/en/governing-platforms-ivir-study-june-2020/) and academia.

In concrete terms, platforms should be required to (source: https://europeanjournalists.org/blog/2020/06/17/common-letter-on-algorithm-transparency-and-data-access-on-content-hosting-platforms/):

- Publish regular (once a year or twice a year) reports on content moderation, ad targeting and ad delivery and human-rights impact assessments. These transparency and accountability reports should not only include quantitative data on content takedowns, but cover explanations and analysis of how the platform deals with illegal content and goods in general. They should follow Commission-set standards that allow comparability over time and across platforms and allows oversight bodies to check breaches of the companies' own policies.
- Make available a comprehensive, meaningful ad archive (see response in section IV, "online advertising")
- Enable data access to third parties (for example civil society organizations, academia, journalists) for public interest scrutiny. Concretely, this would mean institutionalizing privileged data-sharing partnerships and ensuring the content-hosting platforms produce high quality, workable, APIs with data. (cf. https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like).

    - This should allow researchers and regulators to examine the purpose, constitution, and policies around algorithmic or automated decision-making systems, and to interview people who build and interact with different parts of that system, and observe how people use the system.
    - It should also allow researchers and regulators to identify and assess what data was used to train the algorithm, how it was collected, and whether it is enriched with other data sources, and whether that data changed over time.
- Develop, in consultation with relevant stakeholders, including civil society, appropriate guidance for state-of-the-art procedures regarding human rights impact assessment, as recommended by the Council of Europe, as part of human rights due diligence. These procedures should be mandatory with regard to all algorithmic systems with potentially significant human rights impacts.6

These measures should be designed in compliance with the GDPR.

19 What type of information should be shared with users and/or competent authorities and other third parties such as trusted researchers with regard to the use of automated systems used by online platforms to detect, remove and/or block illegal content, goods, or user accounts?
Please see answer to question 18 above.

20 In your view, what measures are necessary with regard to algorithmic recommender systems used by online platforms?
A mandatory transparency and accountability regime for algorithmic recommender systems should be put in place by the DSA. This would help both users and oversight bodies to check and monitor compliance with EU and human rights law.

Users should have easy-to-access and easy-to-understand information on whether and when they are subjected to algorithmic recommender systems. If that is the case, they should be provided with accessible information easily comprehensible language as to what personal behavioral data is being used and basic information about the recommender system. The goal of such information should be to empower users to decide whether they want to find more detailed information, opt out of the algorithmic recommender system and/or challenge algorithmic decision-making.

Platforms should be required to report on their algorithmic recommender systems. This should include information on how content is ranked, in particular the relevant criteria and any changes made to them (above a certain threshold over a specific period of time as ranking algorithms are constantly changing). If their recommended content includes advertising content, they should also provide information on how ad targeting and delivery works, what policies are in place to allow user redress and what policies for notice and takedown are in place. This information should be made available in easy-to-understand, accessible form to the public and in regular reports to researchers and regulators. Oversight bodies should be able to use the reports to assess the compliance of platforms' algorithmic recommender systems with EU and human rights law. Please see the response to question 18 for details on transparency standards.

This information should help establish a baseline for auditing platforms' algorithmic recommender systems to determine whether they conform to legal, human rights and corporate standards.

21 In your view, is there a need for enhanced data sharing between online platforms and authorities, within the boundaries set by the General Data Protection Regulation? Please select the appropriate situations, in your view:

For supervisory purposes concerning professional users of the platform - e.g. in the context of platform intermediated services such as accommodation or ride-hailing services, for the purpose of labour inspection, for the purpose of collecting tax or social security contributions	
For supervisory purposes of the platforms' own obligations – e.g. with regard to content moderation obligations, transparency requirements, actions taken in electoral contexts and against inauthentic behaviour and foreign interference	X
Specific request of law enforcement authority or the judiciary	
On a voluntary and/or contractual basis in the public interest or for other purposes	X

22 Please explain. What would be the benefits? What would be concerns for the companies, consumers or other third parties?
It is important for data sharing to remain limited in scope and duration to prevent it from inadvertently turning into another surveillance layer. As highlighted in the responses to questions 9 and 18, government intervention is necessary to increase data access to study the prevalence and impact of disinformation. However, given the political nature of this question, data analysis should be conducted by a decentralized, GDPR-compliant network of trusted academic and civil society researchers.

Data sharing with authorities to enhance law enforcement in relation to e.g. tax and labor laws should also be limited in scope. For example, an aggregate comparison of tax income implied by the transactions on a platform and actual tax payments can provide insights into whether additional measures are necessary to facilitate tax payments. Access to user-level data should not be given unless it has been shown that this is necessary, suitable and proportionate.

23 What types of sanctions would be effective, dissuasive and proportionate for online platforms which systematically fail to comply with their obligations (See also the last module of the consultation)?
After a period of phasing in and ensuring a common understanding of the rules, financial sanctions would be most effective and proportionate. The rationale is similar to that in the GDPR, but enforcement should be more stringent than observed for the GDPR.

II. Reviewing the liability regime of digital services acting as intermediaries?

6 The E-commerce Directive also prohibits Member States from imposing on intermediary service providers general monitoring obligations or obligations to seek facts or circumstances of illegal activities conducted on their service by their users. In your view, is this approach, balancing risks to different rights and policy objectives, still appropriate today? Is there further clarity needed as to the parameters for 'general monitoring obligations'? Please explain.

We concur with EDRi's position that the prohibition of general monitoring obligations is essential, and we oppose the idea of mandating measures that would lead to an indiscriminate verification and control of all the online content or behavior (see page 23 in https://edri.org/wp-content/uploads/2020/08/DSA-Consultation-Response.pdf).

III. What issues derive from the gatekeeper power of digital platforms?

1 To what extent do you agree with the following statements?

	Fully agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Fully disagree	I don't know/No reply
Consumers have sufficient choices and alternatives to the offerings from online platforms				X		
It is easy for consumers to switch between services provided by online platform companies and use same or similar services provider by other online platform companies ("multi-home")			X			
It is easy for individuals to port their data in a useful manner to alternative service providers outside of an online platform					X	
There is sufficient level of interoperability between services of different online platform companies					X	
There is an asymmetry of information between the knowledge of online platforms about consumers, which enables them to target them with commercial offers, and the knowledge of consumers about market conditions.	X					
It is easy for innovative SME online platforms to expand or enter the market				X		
Traditional businesses are increasingly dependent on a limited number of very large online platforms.		X				
There are imbalances in the bargaining power between these online platforms and their business users	X					
Businesses and consumers interacting with these online platforms are often asked to accept unfavourable conditions and clauses in the terms of use/contract with the online platforms	X					
Certain large online platform companies create barriers to entry and expansion in the Single Market (gatekeepers)		X				
Large online platforms often leverage their assets from their primary activities	X					

(customer base, data, technological solutions, skills, financial capital) to expand into other activities						
When large online platform companies expand into such new activities, this often poses a risk of reducing innovation and deterring competition from smaller innovative market operators		X				

Main features of gatekeeper online platform companies and main relevant criteria for assessing their economic power (p. 30-32)

1 Which characteristics are relevant in determining the gatekeeper role of large online platform companies? Please rate each criterion identified below from 1 (not relevant) to 5 (very relevant):

Large user base	5/5
Wide geographic coverage in the EU	2/5
They capture a large share of total revenue of the market you are active/of a sector	5/5
Impact on a certain sector	5/5
They build on and exploit strong network effects	5/5
They leverage their assets for entering new areas of activity	3/5
They raise barriers to entry for competitors	3/5
They accumulate valuable and diverse data and information	5/5
There are very few, if any, alternative services available on the market	5/5
Lock-in of users/consumers	5/5
Other	

3 Please explain your answer. How could different criteria be combined to accurately identify large online platform companies with gatekeeper role?
There are two main challenges for the criteria: First, they should be MECE (mutually exclusive, collectively exhaustive). The criteria should enable authorities to assess a clearly defined set of platform characteristics. It is preferable to define these as objectively as possible, for instance, strong network effects are easier to assess than lock-in of consumers (which is more likely an amalgam of variables). Besides, they should focus on platform characteristics and not mix them with types of harm created (for example, raising barriers to entry for competitors).

Second, they need to be applicable across markets. This is challenging given the potential application of the gatekeeper criteria in app distribution, news aggregation, general search or even e-commerce. As some form of market coverage/market share is likely to be a key indicator, the latest insights into market definition are central to making sure markets are defined appropriately.

4 Do you believe that the integration of any or all of the following activities within a single company can strengthen the gatekeeper role of large online platform companies ('conglomerate effect')? Please select the activities you consider to steengthen the gatekeeper role:

online intermediation services (i.e. consumer-facing online platforms such as e-commerce marketplaces, social media, mobile app stores, etc., as per Regulation (EU) 2019/1150 - see glossary	X

search engines	X
operating systems for smart devices	X
consumer reviews on large online platforms	
network and/or data infrastructure/cloud services	
digital identity services	X
payment services (or other financial services)	X
physical logistics such as product fulfilment services	
data management platforms	
online advertising intermediation services	X
other. Please specify in the text box below.	

6 Do you encounter issues concerning commercial terms and conditions when accessing services provided by large online platform companies? Please specify which issues you encounter and please explain to what types of platform these are related to (e.g. e-commerce marketplaces, app stores, search engines, operating systems, social networks).
One area where large online platforms can create considerable harm is privacy beyond the scope of the General Data Protection Regulation. While the GDPR asserts a minimum level of data protection, it does not address the conflict of interest between consumers and firms relating to privacy: large platforms have strong incentives to race to the bottom and consumers have no tools to make effective privacy choices. This is worse when consumers deal with large online platforms of all types because consumers do not have any choice. This aggravates concentration dynamics: access to ample behavioral data reinforces the imbalance between competitors because the platforms that offer the consumer-facing product have significantly more insights into consumer behavior.

Most behavioral data should not be collected in the first place because its economic value is not proportionate to the harm it creates. The deep intrusion into privacy is not offset by the little added value created mainly for advertisers, most of which is extracted by the data-collecting platform. The current terms and conditions do not give individuals an effective way to opt out from those practices.

Even for terms and conditions that are not in and of themselves problematic, their lack of accessibility fosters disengagement and increasing distrust. A first necessary, but not sufficient, step is a move towards more meaningful transparency. For instance, terms of services, conditions, privacy statements and, in the cases of social networks, "community guidelines" should be laid out more clearly and easily understandable. Platforms should be required to provide easy-to-understand summaries of the terms and conditions in all EU languages, accessible to all (for example, in "Easy Language" in Germany; audio/video options) and potentially making use of EU-wide icons or symbols.
Especially for social media and search engine companies, the information asymmetry between platforms and users is an issue. Platforms know a lot about their users and, to a certain degree, share this data with advertisers. However, users know very little about the platforms, how they work, how their personal behavioral data is used and what privacy controls they have access to. Some large platforms have taken steps to remedy this issues (for instance, https://www.google.com/search/howsearchworks/?fg=1). Such explanations should be made mandatory to reduce the information asymmetry. They should follow EU-wide standards as to what platforms need to have them, what information needs to be relayed and in what way (accessible, easy-to-understand).

7 Have you considered any of the practices by large online platform companies as unfair? Please explain.

As explained in the answer to question 6, large online platforms have access to large amounts of behavioral data. This allows them to develop dark patterns of many types to nudge consumers to provide more data about themselves and consent to conditions they would have not accepted had they had a better chance of understanding them. Large online platforms undertake A/B testing to assess consumer responses to different designs and can and do use this to engineer their products in their own best interest.

9 Are there specific issues and unfair practices you perceive on large online platform companies?
See answer to question 7.

10 In your view, what practices related to the use and sharing of data in the platforms' environment are raising particular challenges?
There are four main concerns:

First, as mentioned in the answer to questions 6 and 7, platforms are not effectively constrained in their data collection practices vis-à-vis consumers. All large online platforms that monetize through advertising share their user data in real-time auctions. Sharing the data more widely is not a desirable response. Instead, there should be a thorough assessment of how much behavioral data is acceptable to collect in the first place. Once that is established, further remedies can be designed for the behavioral data which is acceptable to collect (e.g. prevention of merging of that data to create individual consumer profiles).

Second, with a view to social media companies, search engines and video portals: The use of personal behavioral data also amplifies existing risks such as the spreading of disinformation and hate speech online. In addition to the harm to privacy, personalizing content to appeal to an individual's emotions has amplified the negative externality of disinformation. Such personalization would hardly be possible without the massive amounts of personal behavioral data have at their disposal. While personalized content can be harmless and benevolent for many users in many cases, it creates serious challenges both for individuals and for societies and democratic processes as a whole, for instance, when the content being pushed is a supposed cure for COVID-19, wrong election dates displayed to certain groups of people or discriminatory, misogynist content.

Third, large online platforms can obtain quasi-regulatory powers over personal data that hamper competition. When those firms decide whether to share personal data and/or enable its collection, privacy may be enhanced, but competition may suffer as a result. Small firms may find themselves shut out because they are unable to compete with the dominant firms in related markets that draw on personal data as an input. Examples of such behavior includes Chrome's announcement that it would phase out third-party cookies by the end of 2021 and Tile's complaint about Apple's restrictions on the use of location data by apps that is more restrictive for third-party apps than for Apple's own apps. In principle, limits on the sharing of personal data are welcome. However, those limits do not improve privacy, and can harm competition if the same data is used without concern within a company but not accessible to external companies, even if they offer privacy standards that are at least as high and provide a service that consumers value.

Fourth, not only consumers, but also businesses that deal on a platform are likely to face an information asymmetry, and not just relating to personal data. Platforms can impose terms that give them access to comprehensive information about the transactions of a business even though the business might prefer to keep that information confidential.

Given the market position of the large online platforms, smaller businesses have no meaningful bargaining power and need to accept the terms.

11 What impact would the identified unfair practices can have on innovation, competition and consumer choice in the single market? (sic!)
As highlighted in the answer to question 10, those unfair practices are likely to hamper competition and, consequentially, innovation and consumer choice. Where large platforms have quasi-regulatory powers regarding the personal data that firms operating in their ecosystem can collect, this can hamper competition without providing better privacy to consumers.

The same applies to the ability of large platforms to impose terms that give them superior access to transaction data. The large platform can be expected to use that data to outcompete smaller businesses in downstream or related markets. This harms competition and limits the ability of other firms to create innovation based on the data despite their contribution to it.

12 Do startups or scaleups depend on large online platform companies to access or expand? Do you observe any trend as regards the level of dependency in the last five years (i.e. increases; remains the same; decreases)? Which difficulties in your view do start-ups or scale-ups face when they depend on large online platform companies to access or expand on the markets?
Startups often depend on large online platforms. It is important to distinguish between two effects: First, in many cases, large online platforms help startups to come to market, e.g. by increasing their reach on a platform or allowing them to use cloud services instead of developing their own infrastructure. Second, however, this limits the options of startups to disrupt markets as they are bound to stay within the limits of the platform they are using. This makes them less likely to be disruptive for large players. Large players, in turn, can often imitate, acquire or, in the worst case, foreclose meaningful competitors.

This dependency is likely to have increased given the reduced number of entries in markets close to the core business of Google, Amazon, Facebook, Apple and Microsoft (GAFAM). If the competition in and/or for the markets that are currently dominated by large online platforms becomes even weaker, business – including startups – that rely on those markets are even more dependent on the increasingly entrenched incumbents.

13 Which are possible positive and negative societal (e.g. on freedom of expression, consumer protection, media plurality) and economic (e.g. on market contestability, innovation) effects, if any, of the gatekeeper role that large online platform companies exercise over whole platform ecosystem?
Gatekeeper platforms have produced large positive benefits by lowering the barriers to enter the markets that they serve compared to the harder-to-search non-platform or even offline markets. These benefits should be preserved as much as possible, alongside positive externalities such as network effects.

Nonetheless, gatekeeper platforms can also disengage consumers from making deliberative choices. It is highly problematic if it gets harder for consumers to see and consider options that the gatekeeper platform does not promote and instead get nudged into believing they get a full and supposedly objective picture of "the market". The widespread activities of the owners of gatekeeper platforms on downstream or related markets mean that gatekeepers have a strong incentive not to provide the best outcome for the consumer (i.e. showing them the product or content that best fits their needs), but

those outcomes favoring the gatekeeper's commercial interests. This has a strong potential to harm competition on those related markets and makes the gatekeeper's position even less contestable.

This applies particularly to information platforms such as social media companies, search engines and video apps: There a considerable negative individual and societal effects of large gatekeeping platforms. As mentioned in the answer to question 10, gatekeeping platforms gather and use massive amounts of personal behavioral data to fuel their algorithmic content moderation machines. While this certainly has positive effects to connect people, share their (political) opinions and organize movements, it has come with serious downsides. Gatekeeper platforms such as social media companies, search engines and video portals, if not kept in check, carry the risk of undermining democratic processes such as citizens' political opinion-formation and elections. This is not only related to issues such as foreign election interference. The measures described for foreign interference, with the goals of undermining trust in democratic institutions, sowing distrust among the populace and amplifying societal tensions, can be and have been used by domestic actors as well. The infrastructure of gatekeeping platforms is not responsible for societal ills such as antisemitism, racism and belief in conspiracy myths, but it does amplify such content in its algorithmic news and information space. Thus, proper oversight mechanism ensuring transparency and accountability for such platforms is essential.

The COVID-19 pandemic has highlighted some of these issues further: the spread of online health disinformation which is a risk for individual and public health; the strong position of gatekeepers in the digital advertising industry (exemplified by many independent public health organizations advertising on large platforms); the weaknesses of traditional journalistic media in the face of the digital ad platforms; the risks for consumer protection related to supposed miracle cures.

14 Which issues specific to the media sector (if any) would, in your view, need to be addressed in light of the gatekeeper role of large online platforms? If available, please provide additional references, data and facts.
The traditional media sector, i.e. legacy papers, magazines and broadcasters, are not in financial trouble only because of the gatekeeper role of platforms. However, the rise of such platforms has accelerated and acerbated the demise of traditional journalistic publishing houses. A necessary re-balancing requires rethinking which functions journalism can and should serve in a democracy. This necessitates a categorization of some online gatekeeper platforms as instrumental in providing citizens with digital spaces for news, information gathering and opinion exchanges, and then imposing additional requirements to ensure plurality of opinion while tackling disinformation. Such categories have been proposed, e.g. in Germany with the "information intermediary" category in the new media regulatory regime (https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/ModStV_MStV_und_JMStV_2019-12-05_MPK.pdf) or in academic writing as public infrastructure (https://s3.amazonaws.com/kfai-documents/documents/7f5fdaa8d0/Zuckerman-1.17.19-FINAL-.pdf; https://knightcolumbia.org/content/from-private-bads-to-public-goods-adapting-public-utility-regulation-for-informational-infrastructure).

Regulation of large online platform companies acting as gatekeepers (p. 34-40)

1 Do you believe that in order to address any negative societal and economic effects of the gatekeeper role that large online platform companies exercise over whole platform ecosystems, there is a need to consider dedicated regulatory rules?

I fully agree

2 Please explain
Ex-ante regulation for gatekeeper platforms is sensible to reduce the potential adverse effects on the economy and the society. Expert reports have confirmed that while traditional competition policy has its merits, its limitations in digital markets include lengthy procedures (during which competitive harm becomes irreversible) and the requirement of culpability. Regulation has the benefit of setting the rules ex ante, so that procedures to ensure adherence to regulation can be shorter and so that firms do not have to be found guilty of anti-competitive conduct before certain rules can be applied to them. The Furman Report to the UK government makes a clear case for such regulation (see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf).

The need for EU-wide regulation is particularly evident regarding information gatekeepers such as social media companies, search engines and video apps. They provide digital communication and media spaces, and thus have a role in societal debates, democratic processes such as elections, and citizens' political opinion formation. While they can assist such democratic processes, serious dangers for democracy arise as well: Disinformation and discriminatory content spread online can considerably infringe upon citizens' basic human right to form their political opinions without interference, and can furthermore negatively affect individual and public health, as is visible in the COVID-19 pandemic.

Continuing to rely only on (criminal law) rules for individual pieces of harmful/illegal content in national legislation is misguided and not sufficient. These laws do not cover the overarching market failures that create the incentives not to tackle disinformation more effectively. Besides, companies should not be left on their own to decide how to trade off online harms and free speech but should be given clear legal guidance on how they should act. This guidance should not enforce decisions on individual pieces of content, but instead focus on the processes for accountable decision-making. Platforms should be held to international human rights standards for their content moderation policies and practices. To check compliance with legal guidelines, independent oversight, free from corporate and government capture, should be in place for information gatekeepers.

Some of the rules could be extended to non-gatekeeper platforms in the longer term. Applying them to gatekeeper platforms first makes sense as they are likely to be the greatest source of potential harm. This requires a careful setup to avoid conflicts between ex-ante regulation and the NCT. However, a certain overlap in scope may be acceptable if there are clear rules on how to navigate them (for instance, it may still be acceptable to run a market-investigation-type intervention in a market in which gatekeeper platforms are subject to ex-ante rules).

3 Do you believe that such dedicated rules should prohibit certain practices by large online platform companies with gatekeeper role that are considered particularly harmful for users and consumers of these large online platforms?
Yes

4 Please explain your reply and, if possible, detail the types of prohibitions that should in your view be part of the regulatory toolbox.
There are two types of behavior we consider particularly harmful that should be considered for inclusion on a deny list:

First, gatekeeper platforms with a conglomerate structure should face higher hurdles for merging data sets including personal data and for using them across services. The GDPR does not specifically address the special dynamics associated with data-dominant firms. However, in dealing with these firms, users are deprived of any meaningful choice. Hence, gatekeeper platforms should be prevented from engaging in excessive data merging across services. The German Federal Court of Justice recently published its detailed judgment in the case Bundeskartellamt v. Facebook which is instructive on the understanding of choice as an objective of competition policy.

Second, gatekeeper platforms should face clearer rules regarding how to treat their own services. Harm can arise especially if a gatekeeper platform gives preferential treatment to its own services if this is not based on criteria that benefit consumers. In the digital world, it is often difficult to distinguish between vertical and horizontal relationships between services because this may depend on the user group (e.g. some may use Google as an entry point for product search and continue to Amazon, while others may start at Amazon directly). Hence, clear criteria need to be developed to distinguish when preferential treatment is problematic. More evidence would be extremely helpful to specify when and what kind of prohibition is useful to balance the harm to competition and the scope for companies to exploit synergies among their services, see the recommendations by the Expert Group to the Observatory for the Platform Economy (see https://ec.europa.eu/digital-single-market/en/news/commission-expert-group-publishes-progress-reports-online-platform-economy).

5 Do you believe that such dedicated rules should include obligations on large online platform companies with gatekeeper role?
Yes

6 Please explain your reply and, if possible, detail the types of obligations that should in your view be part of the regulatory toolbox.
There are two types of obligations we consider particularly helpful that should be considered for inclusion on a list of special obligations for gatekeepers:

First, gatekeeper platforms should provide meaningful transparency and data on their internal workings to authorities, researchers, and, where appropriate, the public. Their important role to the economy and democracy necessitates comprehensive transparency standards that enable society to understand the impact of gatekeeper platforms on markets as well as on political and social debates. For example, gatekeeper platforms should report on their algorithmic recommender systems and their content moderation policies and practices. The platforms' interest in keeping business-sensitive information private needs to be balanced with the significant public interest in understanding their impact. Transparency is also a prerequisite for assessing the platforms' compliance with EU and international human rights law.

Second, gatekeeper platforms should provide both their business and their personal users with data portability the scope of which needs to go far beyond that stipulated in the GDPR, Article 20. Data portability should be continuous, include a broad range of user-specific data and users should be able to move data directly between platforms. Enabling users to port their data between services is important to reduce data-related lock-in e.g. in app store ratings or location history. While more portability may be desirable for platforms without the gatekeeper status in certain markets, lock-in is a greater concern for gatekeeper platforms and they are more likely to have the relevant technical expertise to

implement it. Smaller platforms should be included in the process, however, in order to prevent e.g. standards from being established that would be difficult for them to adopt.

7 If you consider that there is a need for such dedicated rules setting prohibitions and obligations, as those referred to in your replies to questions 3 and 5 above, do you think there is a need for a specific regulatory authority to enforce these rules?
Yes

8 Please explain your reply.
Yes, a dedicated body is necessary, ideally a newly created EU body or, for the time being, a close coordination network of various national oversight bodies including media regulatory authorities, data protection authorities, election/campaign finance bodies and competition authorities.

The oversight body should be as independent as possible to reduce the risk of governmental as well as industry capture, i.e. securing independence from political and corporate influence. Hence, the regulatory authority should probably not be part of a political ministry/DG and should not include corporate and governmental members. An institutionalized coordination mechanism with academic and civil society experts would be helpful as is a coordination mechanism with national member-state bodies.

9 Do you believe that such dedicated rules should enable regulatory intervention against specific large online platform companies, when necessary, with a case by case adapted remedies?
Yes

10 If yes, please explain your reply and, if possible, detail the types of case by case remedies.
We do not see a reason to limit the range of remedies available. These could range from relatively light-touch behavioral remedies such as non-discrimination (with higher requirements than for gatekeepers in general, see answer to question 4) to more intrusive structural remedies including forms of separation. A broad remedy toolbox goes well with a thorough review process.

One remedy we consider particularly interesting is interoperability. Interoperability is not the answer to all challenges across markets, but it could be a justified remedy in markets with particularly entrenched players and strong network effects.

This type of regulatory intervention might become similar to a NCT. In this case, it should be properly defined when which is to be used and how they interact.

11 If you consider that there is a need for such dedicated rules, as referred to in question 9 above, do you think there is a need for a specific regulatory authority to enforce these rules?
Yes

12 Please explain your reply
As highlighted in the answer to question 8, the remit of such a regulatory authority is broader than that of any individual or even combined authority.

13 If you consider that there is a need for a specific regulatory authority to enforce dedicated rules referred to questions 3, 5 and 9 respectively, would in your view these

rules need to be enforced by the same regulatory authority or could they be enforced by different regulatory authorities? Please explain your reply.
It would be sensible to combine the enforcement of these different rules as they are likely to require very similar expertise and powers.

14 At what level should the regulatory oversight of platforms be organised?
At EU level

15 If you consider such dedicated rules necessary, what should in your view be the relationship of such rules with the existing sector specific rules and/or any future sector specific rules?
Sector specific rules should continue in place. If and where the requirements of ex-ante regulation go beyond their scope, they would take priority.

16 Should such rules have an objective to tackle both negative societal and negative economic effects deriving from the gatekeeper role of these very large online platforms? Please explain your reply.
Yes, they should. Societal and economic effects are often interwoven in the context of digital platforms. In order to arrive at coherent rules, it makes sense to address both types of effects together. This is particularly important if it is necessary to trade off certain (short-term) economic benefit against (long-term) societal impact. Such decisions can be made more consistently if they lie within one set of rules.

The importance of societal effects is particularly evident for online gatekeepers that provide media and communication spaces. Even if companies do not create negative economic effects, they can be detrimental to individuals and society. For instance, the way platforms rank and amplify content based on behavioral data and proprietary algorithms can have negative effects for individuals and society, even if no negative economic effects are being felt.

17 Specifically, what could be effective measures related to data held by very large online platform companies with a gatekeeper role beyond those laid down in the General Data Protection Regulation in order to promote competition and innovation as well as a high standard of personal data protection and consumer welfare?
As highlighted in the answers to questions 4 and 6, we suggest that four measures should be considered:

First, data portability needs to be established as a first step towards data mobility. It is reasonable for gatekeeper platforms to provide a higher level of portability as, for competition to evolve, it is more important for data to be freed up from large platforms than from smaller platforms. This would be expected to reduce data-driven lock-in.

Second, higher barriers to internal data-merging should prevent the creation of comprehensive super-profiles. While, in principle, access is the remedy of choice for most data-driven concerns, the scale of behavioral data collection especially by platforms that are gatekeepers providing consumer interfaces should not be expanded through further access. Instead, consumers need to be given more and real choice regarding how data about them is collected and used, and especially so if the firm they interact with has a gatekeeper position.

Third, interoperability and open standards can play an important role in creating a more level playing field for data; however, these are more likely to be suitable for individual areas.

Fourth, transparency and accountability reporting requirements regarding personal data held by companies can enhance consumer welfare by empowering citizens themselves, but also oversight bodies, researchers and journalists to scrutinize corporate data usage. For a more specific instance of this regarding online advertising, see the answers to the questions in part IV.

18 What could be effective measures concerning large online platform companies with a gatekeeper role in order to promote media pluralism, while respecting the subsidiarity principle?
Large online platform companies could pay into an independent fund to support journalism and research (see, for example, https://www.cjr.org/tow_center/google-facebook-journalisminfluence.php; https://www.publicknowledge.org/blog/thepandemic-proves-we-need-a-superfund-to-clean-up-misinformation-on-the-internet/; https://s3.amazonaws.com/kfai-documents/documents/7f5fdaa8d0/Zuckerman-1.17.19-FINAL-.pdf). Many large online platform companies already fund journalism projects, but to minimize the risk of industry capture, an independent fund would be preferable. This fund could be mandated with supporting media pluralism by, among others, supporting local journalism businesses, providing start-up assistance to new ventures, training journalists, supporting research into threats and opportunities of digital journalism as well as into business models for digital journalism.

19 Which, if any, of the following characteristics are relevant when considering the requirements for a potential regulatory authority overseeing the large online platform companies with the gatekeeper role:

Institutional cooperation with other authorities addressing related sectors – e.g. competition authorities, data protection authorities, financial services authorities, consumer protection authorities, cyber security, etc.	
Pan-EU scope	X
Swift and effective cross-border cooperation and assistance across Member States	
Capacity building within Member States	X
High level of technical capabilities including data processing, auditing capacities	X
Cooperation with extra-EU jurisdictions	
Other	X

20 If other, please specify
In addition to the points mentioned in question 19, it is vital to highlight the need for adequate enforcement resources. This not only concerns financial resources, but also expert staff well-versed in a variety of topics and coming from a variety of backgrounds, with a special need for technical expertise. Enforcement is especially important considering the experiences with existing regulatory bodies, which have a vast mandate, but lack budgetary and staff resources, as is the case with data protection authorities.

21 Please explain if these characteristics would need to be different depending on the type of ex ante rules (see questions 3, 5, 9 above) that the regulatory authority would be enforcing?
No, we do not foresee that these would have to differ in principle.

22 Which, if any, of the following requirements and tools could facilitate regulatory oversight over very large online platform companies (multiple answers possible):

Reporting obligation on gatekeeping platforms to send a notification to a public authority announcing its intention to expand activities	X
Monitoring powers for the public authority (such as regular reporting)	X
Investigative powers for the public authority	X
Other	X

23 Other – please list
For the avoidance of doubt, the regulatory authority also needs sanctioning powers. Ample evidence from previous EU-level platform rules such as the Code of Practice on Disinformation show that it is vital for oversight bodies to not only detect breaches and non-compliance, but also enact suitable sanctions.

24 Please explain if these requirements would need to be different depending on the type of ex ante rules (see questions 3, 5, 9 above) that the regulatory authority would be enforcing?
No, we do not foresee that these would have to differ in principle. A potential reporting obligation for gatekeeping platforms that wish to expand their activities should be limited to markets that make use of assets that form part of the central gatekeeper platform (such as data, entry point) and authorities would need to be obliged to react in a very timely fashion. In principle, entry into new markets is desirable, even by gatekeeper platforms, because it often increases competition and consumer welfare. Authorities should have this on top of their mind when designing such an obligation.

25 Taking into consideration the parallel consultation on a proposal for a New Competition Tool focusing on addressing structural competition problems that prevent markets from functioning properly and tilt the level playing field in favour of only a few market players. Please rate the suitability of each option below to address market issues arising in online platforms ecosystems. Please rate the policy options below from 1 (not effective) to 5 (most effective).

	1 (not effective)	2 (somewhat effective)	3(sufficiently effective)	4 (very effective)	5 (most effective)	Not applicable/No relevant experience or knowledge
1. Current competition rules are enough to address issues raised in digital markets		X				
2. There is a need for an additional regulatory framework imposing obligations and prohibitions that are generally applicable to all large online platforms with gatekeeper power					X	
3. There is a need for an additional regulatory framework allowing for the possibility to impose tailored remedies on individual large online platforms with gatekeeper power, on a case-by-case basis		X				
4. There is a need for a New Competition Tool allowing to					X	

address structural risks and lack of competition in (digital) markets on a case-by-case basis						
5. There is a need for combination of two or more of the options 2 to 4.					X	

26 Please explain which of the options, or combination of these, would be, in your view, suitable and sufficient to address the market issues arising in the online platforms ecosystems.
Ex-ante regulation is not suitable to address all actual and potential concerns in digital markets. Hence, in addition to a horizontal regulation, it is important to establish our tools. Our preference is for the NCT to be developed into a flexible tool to investigate and fix structural failures in specific markets. Hence, our answer to question 10 should be read as applying for an NCT as well. Failing this, a case-by-case regulatory approach could be appropriate to address market-specific concerns that fall outside of the scope of competition law.

27 Are there other points you would like to raise?
A systemic challenge of the platform economy is that large, powerful platforms face weak individuals. Consumers have very limited options to make their interests heard (especially where not aligned with those of the platforms). There are only few services that unequivocally act in favor of consumer interests. Such services would be helpful to channel collective action to negotiate with large platforms on the same level. While the development of such services should be done by and in markets, the European Commission can take certain actions to facilitate their emergence.

In particular, strong consumer services may emerge more easily if consumers were able to delegate certain rights. This is apparent for example in the context of data protection and privacy: consumers cannot possibly be expected to have "informational self-determination" if this requires them to manage individual services and data points. Instead, services such as data trusts (see e.g. https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf) could help to give consumers actionable rights vis-à-vis large platforms. This is only possible, however, if consumers can delegate their rights (such as right to give/withdraw consent, to portability) to a trustworthy organization.

IV. Other emerging issues and opportunities, including online advertising and smart contracts

Online advertising

1 When you see an online ad, is it clear to you who has placed the advertisement online?
No

3 What information is publicly available about ads displayed on an online platform that you use?
Basic information on funding source, reach based on certain demographic criteria, time frame of ad.

No information on engagement, no information on who was (not) targeted, very little information on who the ad was (not) delivered to, no detailed information on spending.

Big social media platforms such as Facebook and big platforms using ad exchanges such as Google give users some insights into who is placing an add. In general, however, this is still obscure and/or the information provided by platforms is insufficient. Moreover, verification mechanisms can be circumvented rather easily and there are few sanctioning mechanisms for such behavior, weakening the current transparency system further (cf. Laura Edelson et al., "An Analysis of United States Online Political Advertising Transparency," ArXiv:1902.04385, February 12, 2019, http://arxiv.org/abs/1902.04385; Riley, "This Candidate Does Not Exist," Riley, April 21, 2020, http://posts.walzr.com/this-candidate-does-not-exist).

14 Based on your experience, what actions and good practices can tackle the placement of ads next to illegal content or goods, and/or on websites that disseminate such illegal content or goods, and to remove such illegal content or goods when detected?
For platforms that already have terms of service in place to ban such content, enforcement needs to be enhanced. Platforms should provide transparency on how they enforce their terms of service and if they consistently fail to enforce them, they should be obliged to make their terms of service reflect their actual enforcement behavior in order to prevent users from being misled.

Advertisers also have a responsibility to better screen their ad placements, use exclusion lists and pressure ad platforms to consistently and transparently apply their own terms of service.

15 From your perspective, what measures would lead to meaningful transparency in the ad placement process?
This answer concerns the ad placement process for behavioral advertising (as described in the glossary accompanying this consultation, p. 3), mainly on social media platforms. For this ad placement process, the following measures would lead to meaningful transparency:

1. Mandatory, expanded and vastly improved ad archives: Ad archives can be a valuable tool, especially for researchers and journalists, but their functionality is sub-par. Platforms should be required to offer ad archives with minimum requirements regarding search functions, download options, download speed and accessibility. In addition, more information than currently available is necessary:
    1. Targeting and delivery transparency: Additional data on targeting and delivery, i.e. on the targeted audience and the actual audience, is necessary

to assess if discriminatory practices occur. Information on who was and who was not targeted as well as engagement metrics should be included.
   2. Data source transparency: Ad archives need to allow for more insights into where the data came from that was used to serve ads to make it easier to detect potential privacy violations and discriminatory ad practices.
   3. Financial source transparency: Detailed information on who paid for an ad.
2. Mandatory, expanded transparency reporting on processes for ad targeting and ad delivery: Platforms should be required to report on their policies regarding ad targeting and algorithmic ad delivery mechanisms. Such reports should explain, for example, what data platforms and advertisers can use to target ads, which targeting parameters are prohibited, and why and how accounts can be suspended for violating ad policies.
3. Mandatory, improved ad disclaimers: When users see ads, platforms should be required to provide them with easily accessible and understandable information as to why they were targeted, what other groups saw the ads, based on what data they were targeted (volunteered data, inferred data, lookalike audiences), who funded the ad and how much the ad cost (ranges are acceptable, but need to be narrower than currently is the case). There should be additional information available for interested users, e.g. an easily accessible link to the expanded disclosures in the ad archive.
4. Mandatory advertiser verification: There should be a registry of advertisers in order to require platforms to know their customers and allow users to know who is paying to reach them. Verification processes should ensure that smaller and pop-up advertisers are not put at a disadvantage against bigger advertisers, e.g., through equal-treatment requirements for the verification processes.

Compliance with these requirements should be checked by an independent body (see answer to question 17). Non-compliance should be sanctioned.

16 What information about ads displayed online should be made publicly available?
Since online ads use much more personal behavioral data for their targeting and algorithmic delivery than contextual offline ads, disclosures for online ads need to include much more information than offline (see answer to question 15). Platforms should be required to ensure that ad disclosures are easily accessible and easily understandable. This could be achieved e.g. via common standards for ad disclaimers, for ad archives and transparency reporting.

It is necessary to present information about ads in a suitable way for different audiences: In-feed ad disclaimers are mostly user-facing and should be easily accessible and understandable. They should include information as to why they were targeted, what other groups saw the ads, based on what data they were targeted (volunteered data, inferred data, lookalike audiences), who funded the ad and how much the ad cost (in more narrow ranges than are currently available). There should be additional information available, e.g. an easily accessible link to the expanded disclosures in the ad archive. This ad archive will likely be used by expert researchers who require more and different information than casual social media users (see the answer to question 15, mandatory ad archives).

17 Based on your expertise, which effective and proportionate auditing systems could bring meaningful accountability in the ad placement system?
The first step should be an auditing system for the platforms' transparency reporting (see answer to question 15). These reports should be submitted to a body independent of governments and industry, ideally at the EU level, which is tasked with auditing them. The

body should have enough resources, expertise and sanctioning powers to audit the reports and detect systemic failures by the platforms to (1) respect fundamental rights, (2) adhere to EU law and (3) adhere to their own terms of service.

The next step to make the ad placement system more accountable is by auditing the ad targeting and ad delivery algorithms themselves. To that end, more research on the best process to do this is needed. More data access to platforms will be necessary. The Commission should continue to support algorithmic auditing research and focus parts of this specifically on advertising algorithms.

18 What is, from your perspective, a functional definition of 'political advertising'? Are you aware of any specific obligations attaching to 'political advertising' at a European or national level?
Generally, the transparency requirements mentioned in the answer to question 15 should apply to all ads. However, some member states have specific rules for "political ads", so a distinction will be necessary.

As a working definition, we opt for a broad definition of political advertising covering paid messaging along two axes, advertiser and content.

1. Advertising, no matter the content, is political if it comes from certain advertisers: Political parties, political candidates, political (election) campaigns and lobby organizations.
2. Advertising, no matter the advertiser, is political if it covers certain content: Narrowly speaking, this would be elections/candidates and legislative proposals, yet we call for a broader inclusion of "issue advertising" as well, to cover matters of public interests.

What advertisers and what content is considered "political" is subject to change over time and depends on cultural, language and country differences. Defining a set list should not be left only to private tech companies or the government.

A definition of political advertising should cover all types of media, whether text, images, sound, video or a combination of those, and be encompassing enough to also cover future types of media (for instance, a short while ago, there was no indication that a format such as TikTok videos might be used in paid political communication). Paid political messaging from influencers should be covered in a definition.

Political advertising can happen at all times during the year/legislative period, not just ahead of elections. Thus, rules for political advertising should not only apply ahead of elections. However, during campaign season, additional, stricter rules could be envisioned, such as blackout periods or a freeze in ad volume.

19 What information disclosure would meaningfully inform consumers in relation to political advertising? Are there other transparency standards and actions needed, in your opinion, for an accountable use of political advertising and political messaging?
Because political advertising has the potential to shape political debates, agendas and opinions, it is even more important to create transparency surrounding this paid political communication than it is for commercial advertising. Users and researchers should have access to more, and more detailed, information available on ad targeting and delivery criteria than is currently available.

As a first step, political advertising should be made transparent according to the points raised in the answer to question 15. Additional transparency requirements could be envisioned for political advertising. For example, in order to detect implicit discrimination via advertising pricing, platforms could be required to create transparency as to how they charge different political advertisers differently.

20 What impact would have, in your view, enhanced transparency and accountability in the online advertising value chain, on the gatekeeper power of major online platforms and other potential consequences such as media pluralism?
Enhancing transparency and accountability in online advertising would have a positive impact and is a vital and overdue first step towards an ad value chain compliance regime. However, transparency is not sufficient and further interventions are needed.

The amount and type of personal data collected and used for behavioral advertising targeting should be limited and merging of data from different sources should face additional hurdles. This is necessary to both protect privacy and contain the data-driven power by gatekeeper platforms.

Beyond this, more information needs to be made transparent about the workings of advertising algorithms. Again, transparency reporting would have to be the first step to help regulators, researchers, journalists and citizens understand the online advertising value chain and assess the need for potential intervention.

21 Are there other emerging issues in the space of online advertising you would like to flag?
Online advertising is likely to remain an important source of financing for a range of consumer services. In addition to more transparency and accountability, competitive distortions by unequal access to consumer data should be addressed. This concerns in particular the differential treatment of first-party and third-party data: both Apple and Google have announced plans to make it considerably harder to collect data on their platforms as a third party, which is a very welcome development. However, they still can and do collect data as a first party which they can use for a variety of purposes. This has two effects: First, it reduces the supposed improvements to privacy due to less data collection and sharing. Second, it gives the platforms that set the rules a strong lever to design the rules for data collection in their own favor and to strategically disadvantage competing advertising platforms.

More generally on profiling for ad purposes, existing rules, especially from the GDPR, should be enforced better. National data protection authorities need better financial and personnel resources to fulfill this task.

VI. What governance for reinforcing the Single Market for digital services?

Main issues

1 How important are digital services such as accessing websites, social networks, downloading apps, reading news online, shopping online, selling products online in your daily life or your professional transactions?

Overall	5/5
Those offered from outside of your Member State of establishment	5/5

Governance of digital services and aspects of enforcement

1 Based on your own experience, how would you assess the cooperation in the Single Market between authorities entrusted to supervise digital services?
Cooperation is piecemeal and fragmented. There are many competent regulatory bodies focusing on national, sector-specific questions. Among these are data protection authorities, media regulatory bodies, competition authorities, youth/consumer protection agencies and telecoms regulators (see, for the German case, https://www.stiftung-nv.de/en/publication/regulatory-reactions-disinformation). Better coordination, a clear delineation of competencies and institutionalized communication channels should be established.

2 What governance arrangements would lead to an effective system for supervising and enforcing rules on online platforms in the EU in particular as regards the intermediation of third party goods, services and content (See also Chapter 1 of the consultation)? Please rate, on a scale of 1 (not at all important) to 5 (very important), each of the following elements.

	1 (not at all important)	2	3 (neutral)	4	5 (very important)	I don't know/No answer
Clearly assigned competent national authorities or bodies as established by Member States for supervising the systems put in place by online platforms			X			
Cooperation mechanism within Member States across different competent authorities responsible for the systematic supervision of online platforms and sectorial issues (e.g. consumer protection, market surveillance, data protection, media regulators, anti-discrimination agencies, equality bodies, law enforcement authorities etc.)			X			
Cooperation mechanism with swift procedures and assistance across national competent authorities across Member States			X			
Coordination and technical assistance at EU level				X		
An EU-level authority					X	
Cooperation schemes with third parties such as civil society organisations and					X	

academics for specific inquiries and oversight						
Other: please specify in the text box below						

4 What information should competent authorities make publicly available about their supervisory and enforcement activity?
Regulatory authorities should be free from government and industry capture and legitimized by democratically elected lawmakers. They should report to those lawmakers, with the reports made available to the public, so that especially researchers and journalists can analyze them. These reports should include information on actions taken, sanctions levied, challenges encountered in overseeing large digital platforms, and an overview of emerging issues.

5 What capabilities – type of internal expertise, resources etc. - are needed within competent authorities, in order to effectively supervise online platforms?
Adequate enforcement resources are essential to bring any regulation to fruition. In particular, expert staff needs to come from a variety of backgrounds with a special emphasis on technical backgrounds which tend to be underrepresented.

6 In your view, is there a need to ensure similar supervision of digital services established outside of the EU that provide their services to EU users?
Yes, if they intermediate a certain volume of content, goods and services provided in the EU

7 Please explain
The regulation should make sure not to miss any important services that have chosen not to establish a physical presence in the EU at a specific point in time.

9 In your view, what governance structure could ensure that multiple national authorities, in their respective areas of competence, supervise digital services coherently and consistently across borders?
Coordination mechanisms, for instance in the form of a permanent task force or secretariat, could serve as a governance structure for national authorities.

10 As regards specific areas of competence, such as on consumer protection or product safety, please share your experience related to the cross-border cooperation of the competent authorities in the different Member States.
Specific example of lack of cross-border cooperation in the field of data protection: Data protection authorities from Germany and across Europe criticize lack of coordination in GDPR enforcement, see https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/.

11 In the specific field of audiovisual, the Audiovisual Media Services Directive established a regulatory oversight and cooperation mechanism in cross border cases between media regulators, coordinated at EU level within European Regulators' Group for Audiovisual Media Services (ERGA). In your view is this sufficient to ensure that users remain protected against illegal and harmful audiovisual content (for instance if services are offered to users from a different Member State)? Please explain your answer and provide practical examples if you consider the arrangements may not suffice.
It is too early to fully appreciate the successes and failures of the AVMSD and its governance structure involving ERGA. In any case, it will be crucial to continue providing

resources, in the form of both budgetary support and staff expertise, to ERGA, if this body is to fulfil its task. Enhancing the Commission-sponsored secretariat will help ERGA minimize the risk of government and industry capture.

12 Would the current system need to be strengthened? If yes, which additional tasks be useful to ensure a more effective enforcement of audiovisual content rules? Please assess from 1 (least beneficial) – 5 (most beneficial). You can assign the same number to the same actions should you consider them as being equally important.

Coordinating the handling of cross-border cases, including jurisdiction matters	5/5
Agreeing on guidance for consistent implementation of rules under the AVMSD	5/5
Ensuring consistency in cross-border application of the rules on the promotion of European works	2/5
Facilitating coordination in the area of disinformation	5/5
Other areas of cooperation	

Final remarks

We thank the Commission for the opportunity to participate in the consultation for the DSA. The responses to the consultation questions were written by Aline Blankertz and Dr. Julian Jaursch, with input from colleagues from SNV as well as other European think tank representatives. For questions and comments, please contact the authors Aline Blankertz (ablankertz@stiftung-nv.de) and Dr. Julian Jaursch (jjaursch@stiftung-nv.de). We look forward to engaging further with the Commission and other stakeholders in the future.