VIENNA / 4 September 2020

Consultation response

Commission questionnaire on the Digital Services Act

EPICENTER .WORKS
for digital rights

INTRODUCTION

epicenter.works has published its position on the Digital Services Act (DSA) in the summer of 2019 at https://www.platformregulation.eu. We also contributed to the positioning of our EU umbrella European Digital Rights (EDRi). Part of this response is based on the answering guide and response from EDRi. See https://edri.org/wp-content/uploads/2020/08/DSA-Consultation-Response.pdf and https://edri.org/EDRiDSAAnsweringGuide.html.

Table of Contents

QUESTIONNAIRE RESPONSE

I. How to effectively keep users safer online?

1. Main issues and experiences

A. Experiences and data on illegal activities online

Questions 1-18: no epicenter.works response

19. What actions do online platforms take to minimise risks for consumers to be exposed to scams and other unfair practices (e.g. misleading advertising, exhortation to purchase made to children)? (3K characters max.)

Misleading advertising causes problems in today's online environment that can even affect the integrity of democratic debates. In 2018 Facebook announced their “Paid by” functionality that was meant to counter disinformation and election manipulation with transparency. Several studies found

that this feature was very ineffectively implemented and could easily be circumvented (see sources in EDRi's response https://edri.org/wp-content/uploads/2020/08/DSA-Consultation-Response.pdf).

Similarly, online platforms fail in their mitigation efforts of the negative impact of targeted advertisement. From a consumer perspective it would be necessary to offer effective transparency of the concrete targeting criteria used by the advertiser and offer the data subject control over their advertisement profile.

Question 20: no epicenter.works response

21. Do you consider these measures appropriate?

No

B. Transparency

Questions 1-4: no epicenter.works response.

5. When content is recommended to you - such as products to purchase on a platform, or videos to watch, articles to read, users to follow - are you able to obtain enough information on why such content has been recommended to you? Please explain (3K characters max)

No. Currently platforms fail to provide adequate information to users that explains why certain content appears or does not appear in their feeds. This information inequality between the platform and everyone else proliferates from individual users to public authorities and researchers. Given the huge impact that algorithmic content curation has on media consumption, democratic debates and education, this information inequality is problematic.

Hence, we argue that the DSA should offer users greater transparency and control over the algorithmic curation of the content that is (not) shown to them by social media platforms with a significant market share. At a minimum, settings should offer a fully chronological timeline, but would benefit from including also other options that empower the user to take control of their information diet. Users can should be able to make these decisions actively and also for the duration of individual sessions. The concrete options the platform must offer can be evaluated by a platform regulator, which can issue guidance on potential additions and the design of the feature.

Following a risk based approach, online platforms above a certain global revenue with a dominant market position in several EU countries should be obliged to undertake an impact assessment of their algorithmic curation systems. Additionally, a platform regulator should have the mandate oversee this obligation, to supervise algorithmic curation in general and intervene when media plurality is threatened.

For more information and definitions about algorithmic curation we reference our proposal: https://www.platformregulation.eu/#algorithmic-accountability-and-disinformation

Finally, transparency obligations regarding targeted advertisements need to be stronger than those for organic content that is displayed without financial intervention of the poster. The Facebook functionality "Why Am I Seeing This Ad?" has mostly failed to create meaningful transparency for

individuals, researchers or public authorities. Individuals need to be given the information why exactly they have been targeted with a a particular piece advertisement, which has to include the use of targeted audiences, look-alike audiences, the personal information of them that was used to target them, the true verified name of whoever paid for the ad and any amplification that the platform used to target the person.

For macroscopic transparency from the perspective of researchers, public authorities and civil society watchdogs it would be highly beneficial to establish advertisement archives that need to include all online advertisements from dominant platforms. For more explanation on this point, see our proposal: https://www.platformregulation.eu/#must-advertisement-archive

C. Activities which could cause harm but are not, in themselves, illegal

1. In your experience, are children adequately protected online from harmful behaviours, such as grooming and bullying, or inappropriate content? (3K characters max)

The unattended use of the internet by children bears a number of risks for them, such as grooming by adults, bullying by peers, or the consumption of content that can be considered inappropriate for children. Those online risks mirror similar risks children face in the offline world, and as is the case there, it is primarily the responsibility of a child's guardian (parents, teachers, etc.) to ensure that the children under their care are protected—for example by preventing the use of online platforms that are not explicitly developed for children. For this to work, it is the platform providers' responsibility to clearly state to users whether their online service is available to and safe for children, including the deployment of appropriate protective measures.

On many online platforms, however, including those built for them, children are not sufficiently protected against privacy intrusions and data exploitation. Today's children have the biggest digital footprint of any generation in human history. Sometimes, the collection of a child's data starts even before they are born, and this data will increasingly determine their future (https://www.unicef.org/child-rights-convention/open-letter-to-worlds-children#digital). Third parties that record children's every step not only increase the risk that past actions may later beused against them, but it exposes them to early commercial and political manipulation through micro-targeted advertising (https://www.ugent.be/re/mpor/law-technology/en/research/childrensrights.htm).

The early collection and analysis of children's data can also contribute to social and commercial discrimination. Already today, companies that want to target their products towards children, but also some state authorities, actively seek to record, store and use children's personal data to assess and predict their behaviour.

A Big Brother Watch 2018 report found that the UK "demands a huge volume of data about individual children from state funded schools and nurseries". Data such as a child's name, birth date, ethnicity, school performance, special educational needs and so on, are easily combined with other publicly available information. Local authorities are working with tech giant IBM to train algorithms that predict children's behaviour in order to identify children prone to gang affiliations or political radicalisation. But algorithms portray human biases, for example against people of colour. Reports show that authorities treat children in danger to be recruited by a gang as if they were part of the gang already. Therefore, racial profiling by algorithms can turn into a traumatic experience for a child (https://www.theguardian.com/society/2018/sep/17/data-on-thousands-of-children-used-to-predict-risk-of-gang-exploitation and

https://www.independent.co.uk/news/education/education-news/teachers-forced-to-act-as-front-line-storm-troopers-to-spy-on-pupils-under-guidelines-aimed-at-10158043.html).

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

Online platforms can easily be manipulated by foreign governments or other coordinated groups to spread divisive messages:

No Reply

To protect freedom of expression online, diverse voices should be heard:

Fully Agree

Disinformation is spread by manipulating algorithmic processes on online platforms:

No Reply

Online platforms can be trusted that their internal practices sufficiently guarantee democratic integrity, pluralism, non- discrimination, tolerance, justice, solidarity and gender equality:

Fully disagree

3. Please explain. (3K characters max)

It is vital for democratic discourse that freedom of speech is upheld. These protections are particularly relevant for challenging speech that is sometimes even regarded as offensive or disturbing (see ECHR 5493/72). Therefore, any efforts to curtail the spread of legal speech or use criminal law to tackle the problem of disinformation are hugely problematic from a fundamental rights perspective.

Furthermore, the content moderation practices of the biggest online platforms have an overwhelmingly negative track record of intentional and unintentional infringements of freedom of speech. The internal processes of global technology companies are ill-equiped to handle the complicated and culturally and legally contextualised questions of freedom of speech. Furthermore as for-profit entities they don't have the right incentives to make balanced decisions about regulating speech. Most legislation in the area of content moderation created only one-sided incentives for overblocking. Instead of focusing on more deletion of content, the purpose of good content moderation legislation should be to increase the quality of the content moderation that is already happening while strengthening the rule of law and the legal system.

Question 4 and 5: no epicenter.works response.

D. Experiences and data on erroneous removals

1. Are you aware of evidence on the scale and impact of erroneous removals of content, goods, services, or banning of accounts online? Are there particular experiences you could share? (5K characters max)

A comprehensive evaluation of the content removal practices of dominant online platforms is currently not possible. Without meaningful transparency about all content moderation practices such

a debate is fruitless. The DSA should introduce strong transaprency obligations that allow independent researchers, public authorities and affected groups to gain a better understanding of the content moderation practices on dominant platforms.

The transparency reports should be published monthly and include

- a summary of the actions taken to establish an effective notice and action system and a description of the internal organisation of this system,
- the number of the received notifications of potentially illegal or ToS-infringing content and their geographical and language localisation,
- a summary the actions taken and on which ToS paragraph or legal basis those actions are based,
- statistics on the time spent by personnel on each case, the education of this personnel, their geographical location, cultural background and language skills,
- a summary of all fully or partially automated systems that are used in the content moderation system.
- A platform regulator should have the competence to issue binding public guidelines which detail the requirements for transparency reports and their methodology. The purpose of these guidelines is to enable comparability between manual and automated processes, to prevent discrimination of protected groups and to ensure the validity of the collected data. If the transparency report is called into question, the regulator should be empowered to conduct an external audit to ensure their validity. The regulator should be inclusive in the creation of the guidelines and take the utmost account of the input from researchers, public authorities, civil society and affected platforms.

In case partly or fully automated systems play a role in content moderation, they need to undergoe a constant impact assessment which should be part of the transparency reporting.

Questions 2-7: No epicenter.works response

8. Does your organisation access any data or information from online platforms?

*** Yes, data regularly reported by the platform, as requested by law**

Yes, specific data, requested as a competent authority

Yes, through bilateral or special partnerships

On the basis of a contractual agreement with the platform

*** Yes, generally available transparency reports**

Yes, through generally available APIs (application programme interfaces)

Yes, through web scraping or other independent web data extraction approaches

*** Yes, because users made use of their right to port personal data**

Yes, other. Please specify in the text box below

No

9. Please indicate which one(s). What data is shared and for what purpose, and are there any constraints that limit theseinitiatives? (3K characters max)

For the creation of our position on platformregulation.eu we assessed the transparency reports and other publicly available informations about the content moderation practices of platforms, as well as the personal data accessible due to GDPR requirements. The understanding we could gather with these tools was very limited and unsatisfactory for our purposes as public watchdog.

Question 10: no epicenter.works response

11. Do you use WHOIS information about the registration of domain names and related information?

***** Yes

No

I don't know

12. Please specify for what specific purpose and if the information available to you sufficient, in your opinion? (3K characters max)

We sometimes use WHOIS to verify the authenticity and ownership of domain names. The non-personal information contained therein (reduced as a consequence of GDPR) is sufficient for this purpose. In any event, in cases of criminal behaviour we would inform law enforcement authorities who have the ability to obtain subscriber information, through due process, should an investigation be in order.

13. How valuable is this information for you? (Please rate from 1 star (not particularly important) to 5 (extremely important))

***** 3

14. Do you use or ar you aware of alternative sources of such data? Please explain. (3K characters max)

No.

Section 1: no epicenter.works response.

2. 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.

Maintain an effective 'notice and action' system for reporting illegal goods or content:

Yes, only by larger online platforms

Maintain a system for assessing the risk of exposure to illegal goods or content:

Such measures should not be legally required

Have content moderation teams, appropriately trained and resourced:

Yes, only by larger online platforms

Systematically respond to requests from law enforcement authorities:

Such measures should not be legally required

Cooperate with national authorities and law enforcement, in accordance with clear procedures:

Yes, by all online platforms, according to the activities they intermediate (e.g. content hosting, selling goods or services)

Cooperate with trusted organizations with proven expertise who can report illegal activities for fast analysis ('trusted flaggers'):

Such measures should not be legally required

Detect illegal content, goods or services:

Such measures should not be legally required

In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law:

no epicenter.works response

Request professional users to identify themselves clearly ('know your customer' policy):

Such measures should not be legally required

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):

no epicenter.works response

Inform consumers when they become aware of product recalls or sales of illegal goods:

no epicenter.works response

Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities:

Such measures should not be legally required

Be transparent about their content policies, measures and their effects:

Yes, by all online platforms, according to the activities they intermediate (e.g. content hosting, selling goods or services)

Maintain an effective 'counter-notice' system for users whose goods or content is removed to dispute erroneous decisions:

Yes, by all online platforms, according to the activities they intermediate (e.g. content hosting, selling goods or services)

2. Please elaborate, if you wish to further explain your choices. (5K characters max)

Law enforcement authorities should not be allowed to send requests to online platforms outside of the appropriate legal framework involving courts or other independent judicial authorities such as the use of the notice and action (N&A) mechanism to flag potentially illegal content. Instead, when law enforcement agencies find potentially illegal online content or behaviour online, they should go through proper due process channels. This is because when public authorities restrict fundamental rights by using their formal powers (e.g. to demand the removal of online speech or prosecute suspects), their powers are and should be limited by due process safeguards prescribed by law. Allowing law enforcement officers to use the N&A mechanism would systematically bypass those safeguards. What is more, research has shown that content removal requests by police are four times more likely to be successful than other users' requests—indicating that platform operators either reduce the thoroughness of their own verification when removal requests come from police officers or just blindly trust that law enforcement officers make no mistakes. This kind of anticipatory obedience by platform operators increases the risk of abuse and politically motivated censorship. When issuing an order to remove or block access to an illegal piece of content, law enforcement should therefore require prior judicial authorisation by a court or an independent judge.

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

* Precise reason why the activity is considered illegal

* Description of the activity

* Identity of the person or organisation sending the notification. Please explain under what conditions such information is necessary:

* Other, please specify

4. Please explain (3K characters max)

A valid notification should be sufficiently precise and adequately substantiated. This should include

1. the location of the content (URL);
2. the reason for the complaint (potentially including legal basis under which the content has to be assessed);
3. evidence of the claim and potentially legal standing;
4. a declaration of good faith that the information provided is accurate
5. considerations on limitations, exceptions, and defences available to the content provider.

Only in notifications of violations of personality rights or intellectual property rights should the identification information of the notifier be mandatory. In all other cases, identification and contact information of the notifier should be optional.

5. How should the reappearance of illegal content, goods or services be addressed, in your view? What approaches are effective and proportionate? (5K characters max)

There needs to be a distinction between platforms for the sharing of goods and services, which have many automatic or manual means for this purpose at their disposal, and content sharing platforms. For the latter freedom of speech and privacy considerations have to be taken into account. In this context, notice and staydown procedures are inherently linked to monitoring obligations for the platform that would be a disproportionate burden and serious infringement on users' rights to privacy and freedom of speech. Many types of content that courts have found to be illegal can be recontextualised as parody, journalism, or pastiche and suddenly become protected by freedom of speech. Algorithmic content filters/detection are always blind to the context of speech. This limitation applies to all forms of content, but in particular to text.

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? (3K characters max)

Automated tools for the detection or removal of content should never be mandated by law.

Platforms relying on such automated tools record a much higher amount of wrongful takedowns and poor content moderation decision quality. Not only are algorithms inherently blind to the context of speech (parody, pastiche), the technology itself often produces many false positives that with a high enough number of cases produce unacceptable infringements of freedom of speech. Currently there is no technology that can fulfil the obligations such decision making would entail. Mandating by law a technology that does not exist is wishful thinking and not evidence based policy making.

For example, in 2017, the pop star Ariana Grande streamed her benefit concert "One Love Manchester" via her YouTube channel. The stream was promptly shut down by YouTube's upload filter, which wrongly flagged Grande's show as a violation of her own copyright. The same automated tools remove people's private recordings of classical music from Bach to Beethoven, claiming they violated someone's copyright. They remove thousands of YouTube videos that could serve as evidence of atrocities committed against civilians in places like Syria, potentially jeopardising any future war crimes investigation that could bring war criminals to justice.

Because of their contextual blindness or, in other words, inability to understand users' real meaning and intentions, automated tools often flag and remove content that is completely legitimate. Thus, journalists, activists, comedians, artists, as well as any of us sharing our opinions and videos or pictures online risk being censored because internet companies are relying on these poorly working tools.
In another striking example, as the COVID-19 crisis broke out, health guidelines forced big social media companies to send their content moderators home. Facebook's automated "anti-spam" system kicked in and – just like on other social media platforms – started removing crucially important information about the pandemic from trustworthy sources as violations of the platforms' community guidelines. This period perfectly demonstrates why relying on automated processes is often detrimental to the freedom to receive and impart information and democratic debates and processes and should therefore not be required by law. (See: https://blog.witness.org/2020/03/as-content-moderators-go-home-content-could-go-down/)

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?

a) Digital services established outside the Union should fall under the DSA just as much as those established inside the Union.

b) no epicenter.works response.

8. What would be appropriate and proportionate measures that digital services acting as online intermediaries, other than online platforms, should take – e.g. other types of hosting services, such as web hosts, or services deeper in the Internet stack, like cloud infrastructure services, content distribution services, DNS services, etc.? (5K characters max)

Services that do not host but only cache, transmit user-generated content, or facilitate its transmission (such as DNS services, cloud fronting services and peer-to-peer messaging services for example) should not be held liable for user-generated content.

Hosters, cloud providers or CDNs should only be liable once a court has found content on their system to be illegal and they failed to act. They should not be held liable for failure to pro-actively search for or remove content that has not been declared illegal by a court. Platform operators are not the judiciary. Giving them the power (or creating a legal obligation for them) to behave as if they were the judiciary

(a) undermines the institutional and legal order of our democracy, and

(b) cements the quasi-monopolistic position that many of these platform operators already occupy today.

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? (5K characters max)

A sufficiently funded, independent European regulatory entity that is tasked with the enforcement of DSA would be a major factor in tackling illegal activities online. Such a platform regulator is imperative to ensure that the provisions of the DSA are actually enforced in practice. The experience of the GDPR and TSM regulation provide us with sufficient evidence to identify the shortcomings of existing enforcement models. Only a strong, central European agency has the independence and transparent operation to supervise procedural obligations established by the DSA. Such an entity would of course be invited to strongly cooperate with data protection authorities on questions of data protection and media regulators on questions of media plurality, but ultimately the EU agency needs to be in charge of enforcement procedures with the capability of issuing penalties based on a percentage of global revenue. If such an enforcement structure is not achieved in the Commission's proposal for the DSA, the new rules may never be enforced in practice.

Additionally, the DSA should create the possibility for civil society and consumer protection organisations to launch class action lawsuits against dominant platform operators. In cases where regulatory scrutiny is not sufficient to tackle sustained problems in the platform economy, public watchdogs can bring cases in the public interest. With the advent of the GDPR we have seen a surge of strategic litigation activity in the digital rights field. The DSA could also bring about a surge of cases that help enforce the law in practice. Yet, it is important to note that a newly crated EU-wide regulatory entity is the preferred option to ensure that the important decisions are made.

Lastly, all public authorities, civil society, and researchers are currently suffering from a lack of evidence of the practices of dominant online platforms. Smaller platforms like newspaper forums with user-generated content have already participated in research projects and generated valuable insights. However, the most influential platforms in the online economy have so far refrained from opening their data sets and processes to public scrutiny. The DSA should establish a mechanism that public interest research can access the data sets of dominant online platforms. Privacy and ethical standards need to be uphold in the process. See our proposal for details: https://www.platformregulation.eu/#discuss-scientific-access-to-dominant-platforms-via-committee-safeguard

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? (5K characters max)

Legal but potentially harmful speech should only be approached with the utmost caution in the DSA. Such legal speech falls under fundamental rights protections and hence few legal requirements on part of the platform can be deemed reasonable.

Nevertheless, the quality of content moderation practices with regard to legal speech that is potentially ToS-infringing could be drastically improved if these practices fell under DSA provisions on transparency reporting obligations and procedural safeguards of the notice-and-action framework (counter-notifications, redress, etc.).

Additionally, documents such as Terms of Service (ToS) or Community Guidelines that provide the contractual basis of the moderation practices of legal content should follow minimum requirements for transparency and accountability. These should include international human rights standards as well as standards for predictability and need to be appropriate, proportionate and predictable. Users

need to be able to understand in clear language under which rules a given platform operates, how to abide by those rules, and what happens if users break them. For the dominant online platforms the platform regulator should have to approve any changes to these rules ex-ante.

See for further information:

https://www.platformregulation.eu/#recommended-develop-minimum-standards-of-tos-transparency-and-accountability

https://www.platformregulation.eu/#recommended-social-media-oversight-council

https://www.platformregulation.eu/#recommended-enforcement-via-european-platform-regulator

11. In particular, are there specific measures you would find appropriate and proportionate for online platforms to take in relation to potentially harmful activities or content concerning minors? Please explain. (5K characters max)

See the answer to question 10 above. Additionally, platforms should clearly indicate whether they are safe to use for minors.

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.

5 Transparently inform consumers about political advertising and sponsored content, in particular during electoral periods

3 Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with users' complaints

3 Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives

5 Transparency tools and secure access to platforms' data for trusted researchers in order to monitor inappropriate behaviours and better understand the impact of disinformation and the policies designed to counter it

5 Transparency tools and secure access to platforms' data for authorities in order to monitor inappropriate behaviours and better understand the impact of disinformation and the policies designed to counter it

4 Adapted risk assessments and mitigation strategies undertaken by online platforms

1 Ensure effective access and visibility of a variety of authentic and professional journalistic sources

5 Auditing systems over platforms' actions and risk assessments

5 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 manipulation and amplification of disinformation.

5 Other, please specify

13. Please specify:

Although transparency and access to research data for academics and authorities is important, it is even more important not to forget that misinformation online is often not illegal (and should not be). Platforms have the right to look for and remove bot accounts and remove accounts and content that spread hate and lies, but they must do so transparently and consistently. However, no law should mandate any platform to delete incorrect information, and no public authority should get the power to decide what is true and what is false. Platforms and public authorities should not become legally mandated arbiters of truth.

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? (3K characters max)

International human rights law puts very strict requirements for the conditions under which states can restrict freedom of expression and information (such as the principles of legality, necessity and proportionality, legitimacy). According to Article 15 of the European Convention of Human Rights, in emergency situations, states can derogate from their obligation in relation to freedom of expression and information but must justify such derogation by meeting two essential conditions:

(1) The situation must amount to a public emergency that threatens the life of the nation or war; and

(2) the state must have officially proclaimed that state of emergency and notified other countries through the Secretary General of the Council of Europe.

In addition, every measure must be strictly required by the exigencies of the situation.

15. 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).

5 High standards of transparency on their terms of service and removal decisions

5 Diligence in assessing the content notified to them for removal or blocking

5 Maintaining an effective complaint and redress mechanism

5 Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended

5 High accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts

3 Enabling third party insight – e.g. by academics – of main content moderation systems

5 Other. Please specify

16. Please explain. (3K characters max)

Beyond content moderation and transparency best practices, platforms should give their users fine-grained control over what they see – that control should override any business interest a platform

may have in distributing certain content. This includes a right for users to switch off personalised/micro-targeted content and advertising.

Users should also be able to actively curate their own content, which enhances personalisation. One way to achieve it is to open content curation services/tools for competition and enable independent operators (with their own models and algorithms) to plug-in. That way, users could, for instance,receive a non-curated message stream or timeline from their social network and combine it with a third-party curation software offered by, say, a newspaper, European tech company, or civil society organisation they trust.

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? (5K characters max)

The first pillar for addressing the fundamental rights concerns in the current online environment is a strengthening of competition mechanisms with regard to the big tech monopolies. These should include new metrics for assessing harmful market concentration like holistic privacy impact assessments along value chains, a reform of the targeted online advertisement ecosystem and most importantly interoperability to create competition for dominant online platforms.

The second pillar should be the protection of the current liability safe harbour regime for user-generated content. Any increased liability for user-generated content or the establishment of certain duties of care risks serious threats to freedom of speech, freedom of assembly and freedom to conduct business. Without the liability safe harbours, over-removal of legitimate speech by big tech companies is inevitable. Privatising the legality assessment of online expression cannot be the solution. Instead, the EU should improve access to the justice system.

Any attempts to train algorithms to favour or protect content based on categories of gender or discriminated group requires training algorithms explicitly aware of those categories. This express awareness could be used in both both to favour and to disfavour such content, and can easily lead to suppression of vulnerable groups or political unfavourable content in certain parts of the world.

The third pillar is an update to the notice-and-action regime.

1. Notifications should offer categories of different types of violations, ranging from various classes of illegal content to legal content that might be in breach of the Terms of Service or other rules of the platform. Different notification categories should trigger different procedures, which take into account the fundamental rights of all parties in question, meaning that procedures with stricter safeguards cannot be substituted by procedures with less strict ones. For example, a notification of illegality with the possibility of legal redress cannot be circumvented by deletion of the content in question under the Terms of Service of the platform.
2. A valid notification should be sufficiently precise and adequately substantiated. Only in notifications of violations of personality rights or intellectual property rights is the identification information of the notifier mandatory. In all other cases, identification and contact information of the notifier are optional.
3. For purposes of procedural fairness and increasing the quality of content moderation, the content provider should be informed about a notification of his or her content, the reason for

the notification, information about the subsequent process and possible ways to appeal or file a counter-notifications. The content provider should be informed immediately once the platform has received the notification and not just after a decision has been taken. Exceptions from this obligation to notify the content provider might apply only if sending notifications would hamper ongoing law enforcement investigations.

4. Possibility for counter-notification should be offered to the content provider to respond to the claim of the original notifier with evidence and arguments to the contrary. This counter-notification should be an option even before a decision by the platform is taken. Both original notification and counter-notification should apply the same standards in terms of declarations of good faith. The counter-notification can also be filled after the content has already been removed and can also challenge the category of the content in question.
5. Online Platforms have to inform the parties involved in notification about the outcome of the decision a platform has taken in their case. This communication is always sent to content providers and to notifiers if they have provided contact details in their notification.
6. Online platforms need to publish information about their procedures and time frames for intervention by interested parties.

See: https://www.platformregulation.eu/#must-procedural-safeguards-for-content-notifications

The fourth pillar is effective legal redress. Both parties of a content dispute (the poster and the notifier) should have avenues for redress against the decision of the online platform. For legal content that might potentially infringe the ToS the redress should take the form of a review by a multi-stakeholder social media council (see: https://www.platformregulation.eu/#recommended-enforcement-via-european-platform-regulator). For potentially illegal content, the redress should take the form of a review by a public dispute settlement body. The decisions by this body should allow for access to the normal legal system to follow up with a redress through the court. It is important that this avenue is also available to the poster.

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. (5K characters max)

See our answer on transparency reporting on question I.1.D.1 and our answer on procedural safeguards in the previous question.

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? (5K characters max)

The source code and training data of such tools should be made available to trusted third parties. As these systems have a vital role in the governance of our democratic debates, media landscape and e-commerce, we need to be able to have an informed debate about how they work in practice and what impact they have on society. The many cases of over-blocking and problematic content moderation

decisions have lead to frequent public outcries. Without a sound understanding of how these systems work, a factual debate is not possible. The feeling of powerlessness in large parts of society needs to be countered by informed decisions about the real workings of algorithms that moderate our discussions.

This level of transparency should be accompanied by regular algorithmic impact assessments, which the platform should be required to conduct of their systems. These assessments should have to be part of the regular transparency reports the platform has to publish.

20. In your view, what measures are necessary with regard to algorithmic recommender systems used by online platforms? (5K characters max)

Minimum transparency requirements should

(1) empower users and return to them the agency and control over information they view on online platforms,

(2) enable public oversight authorities to fulfil their monitoring function over content recommendation systems in order to ensure the systems' compliance with the protection of fundamental rights.

(1) Measures aimed at reinforcing user control should ensure that:

- Users are able to access their full profiling data (including information about and deduced from their online behaviour) in a comprehensible format, including data about and inferred from their behaviour and generated by the platform's algorithms. Existing data protection rules should be complemented with the DSA by addressing the current lack of accessibility and readability of such data. Such behavioural and inferred data fall under the GDPR and therefore data subjects must be able to have this rectified or deleted if they so wish.

- Users are always informed when they are being subjected to algorithmic recommender systems. Explanations of the algorithmic recommender systems should always be accessible and presented to users in tangible and comprehensible language, including information about the family of models, input data, performance metrics and how the model was tested. Such an explanation will allow users to contest the algorithmic decision-making and/or to opt out of it.

- Users always have the right to opt out/switch off the use of such recommender systems, for example on video sharing platforms: which video to watch next; or on marketplaces: which product to buy. In particular, the DSA should guarantee that users' default settings are set as "opt-out" and require them to proactively opt in to personalised content recommendation systems. Platforms should design consent and privacy policies in a way that facilitates informed users' choice.

(2) Measures guaranteeing an effective oversight by competent authorities should ensure that:

- The oversight authority with the power to enforce the DSA are able to audit and assess the functioning of and respect of fundamental rights by algorithmic recommender systems.

Question 21: no epicenter.works response.

22. Please explain. What would be the benefits? What would be concerns for the companies, consumers or other third parties? (5K characters max)

This question's phrasing is unclear. What exactly is the definition of enhanced data sharing? Why is this given as an equal option to access to platform data by law enforcement agencies, which already have the power to access this data subject to due process safeguards?

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)? (5K characters max)

Similar to the GDPR, the maximum penalties for failure to comply with the provisions of the DSA should be calculated as a percentage of the global revenue of the company. This approach creates proportionality among, and dissuasiveness for very large and very small platforms. Nevertheless, not all obligations of the DSA should apply equally to all platforms or entail the risk of penalites. Proportionality in this sense means that the strongest obligations should only apply to the largest platforms and the lowest obligations should apply to small startups and community projects. The challenge of the DSA is to adhere to this proportionality principle for all categories in between without disincentivising platform growth.

Question 24: no epicenter.works response.

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

Question 1: no epicenter.works response.

2. The liability regime for online intermediaries is primarily established in the E- Commerce Directive, which distinguishes between different types of services: so called 'mere conduits', 'caching services', and 'hosting services'. In your understanding, are these categories sufficiently clear and complete for characterising and regulating today's digital intermediary services? Please explain. (5K characters max)

From the users' perspective, the regime set by Articles 12 to 15 of the Directive has a major impact on the level of freedom of expression, freedom of information, right to privacy and personal data protection on the Internet, as well as on the due process of law. From the intermediaries' perspective, it must ensure the needed legal certainty to run their activities. The lack of clarity and precision of the current regime does not allow adequate protection of human rights and the rule of law, nor does it ensure legal certainty for intermediaries.

In order for the EU to respect its current obligations with regard to its own Charter of Fundamental Rights and its upcoming obligations under the European Convention on Human Rights, EDRi underlines the need to revise the current intermediaries liability regime as follows:

- Where an intermediary is not hosting the content (acting as a mere conduit, an access provider or a search engine), it should have no liability for this content, nor should it have general monitoring obligations or obligations to employ proactive measures with regards to this content as an access provider.
- Where an intermediary acts as a hosting provider, its liability with respect to the user-generated content it hosts should be restricted to a lack of compliance with a court order to take down this content. This should not prevent hosting providers from removing content based on their terms and conditions.
- Intermediaries should have no legal obligation to monitor content.

3. Are there elements that require further legal clarification? (5K characters max)

Yes, the lack of clarity around the E-Commerce Directive's liability exemption often leads to a weakening of fundamental rights guaranteed by the European Convention on Human Rights and the European Charter on Fundamental Rights.

A first element of the liability regime that requires legal clarification is the concept of "actual knowledge". At the moment, it is not always clear whether the "actual knowledge" standard refers to the platform knowing that there is allegedly infringing material on their system or knowing for certain that that material is actually illegal (which in many cases is impossible to know with certainty unless a court has taken a decision). This term has therefore been subject to different interpretations of the level of awareness of service providers necessary to trigger the obligation to "expeditiously" remove the content in question, or else face legal liability.

In particular, national lawmakers and judges have faced the difficulty of determining how a hosting provider could obtain actual knowledge of the illegality of a given content without being presented with a court order. While sometimes, the question whether a given piece of content is illegal is relatively easy to answer, most of the time even lawyers need to conduct complex legal assessments (and could still disagree) to determine the legality of, say, an aggressive social media post or a threatening online video. Online platform providers are not only badly equipped to take those complex decisions, they should also not replace our judiciary. Empowering private (often non-EU) companies to be judges of what is legal on the internet seriously undermines the rule of law. That is why, in the absence of a valid decision by a national judicial authority like an ordinary court or judge, intermediaries should not be required by law to assess the legality of user-generated content or be held legally liable for it. This does not preclude platforms' responsibility for their own actions such as the promotion, demotion, or micro-targeting of user-generated content.

A second element that requires legal clarification is potentially conflicting sectoral legislation. Since the entry into force of the E-Commerce Directive, the liability exemption has been undermined by vertical legislation, such as the Copyright Directive, the pending Terrorist Content Regulation, as well as by the encouragement of "voluntary" arrangements, such as the EU Code of Conduct on Hate Speech and the Code of Practice on Disinformation. All of those increase the legal risk for liability of platform providers and users. At the same time, in its Communication "Tackling Illegal Content Online" the European Commission tries to reassure companies that proactively searching for potentially illegal content does not imply knowledge of any illegal content—and therefore does not lead to legal liability. This has created an important confusion and legal uncertainty.

EU legislation such as the upcoming Digital Services Act should therefore protect and uphold the liability exemption as enshrined in the E-Commerce Directive for all types of intermediaries:

- Where an intermediary is not hosting user-generated content (acting as a mere conduit, an access provider or a search engine), it should not be held liable for this content, nor should it have general monitoring obligations or obligations to employ proactive measures with regards to this content as an access provider.
- Where an intermediary acts as a hosting provider, its liability with respect to the user-generated content hosted should be restricted to its lack of compliance of a court order declaring a given content illegal and requiring its removal. This should not prevent hosting providers from removing content based on their terms and conditions.
- Intermediaries should have no obligation to generally monitor online content.

4. Does the current legal framework dis-incentivize service providers to take proactive measures against illegal activities? If yes, please provide your view on how disincentives could be corrected. (5K characters max)

The liability exemption provided by the E-Commerce Directive is widely recognised as one of the key factors that protects freedom of expression and access to information, and allows the internet economy to flourish since its early days. Although the internet and services built on top of it have changed tremendously since then, the general idea of linking liability for online content primarily to the content creator or uploader is still today a cornerstone of freedom of expression and the responsibilities it entails. Without this secondary liability exemption, over-blocking of legitimate content and censorship of users' speech would happen systematically. The liability exemption also prevents a situation in which intermediaries would effectively be forced to scan every single piece of content uploaded on their systems and assess its legality before making it available — and thereby become global arbiters of what is legal and what is not which would create important chilling effects on a number of fundamental rights. Already today, content moderation practices on the biggest platforms show that private companies are badly positioned to do this kind of task well, with an extremely negative impact on both the protection of victims of illegal content and freedom of expression.

The current legal framework could disincentivise providers to actively look for illegal content if they are considered to have "actual knowledge" once they do it. That is why the DSA should clarify that any voluntarily applied content moderation activities do not automatically constitute "actual knowledge" and therefore would not trigger liability in case content is overlooked that is eventually declared illegal by a court. This should be clearly spelled out rather than hidden in a vague "duty of care" regime that opaquely threatens platform operators with liability if they are not "doing enough" to proactively monitor, judge, and remove potentially illegal user and third party content. Such "duty of care" regimes often take the form of political pressure on platforms to take formally voluntary measures without clear and understandable obligations and predictable sanctions for failure to comply with them.

5. Do you think that the concept characterising intermediary service providers as playing a role of a 'mere technical, automatic and passive nature' in the transmission of information (recital 42 of the E-Commerce Directive) is sufficiently clear and still valid? Please explain. (5K characters max)

The distinction between 'active' and 'passive' intermediaries is based on how the internet looked like in the 1990s and 2000s. Today, it has become hardly workable. With the exception of mere conduit services (which should not have any 'duty of care' or secondary liability anyway), almost all modern online intermediaries are active to some degree. The Digital Services Act should therefore not maintain the distinction between active and passive intermediaries and rather focus on the types of services an intermediary offers as well as on the strict enforcement of legal obligations such as transparency, privacy and data protection.

In its recent opinion on the cases C-682/18 Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH and C-683/18 Elsevier Inc. v Cyando AG (available at: http://curia.europa.eu/juris/documents.jsf?num=C-682/18), the Advocate General of the Court of Justice of the European Union (CJEU) specified that a service provider should only be considered as playing an active role and thus as obtaining 'actual knowledge of illegal activity or information' when that knowledge relates to specific illegal information. The mere fact that an intermediary:

- gives access to content hosted on its platform that users access through purely technical and automated means (para. 155);
- does not present third-party content as its own (para. 156);
- classifies and categorises content, allows users to search specific content via a search function and recommends content according to previous search results (para. 156-160);
- bases its business model on online advertising (para. 163-165) and;
- puts in place (automatic) systems to detect illegal activities on its platform (para. 166);

should not lead to the loss of liability exemption under Article 14 of the E-Commerce Directive. The Advocate General's reasoning is just as true for the DSA: "Otherwise, there would be a risk of platform operators becoming judges of online legality and a risk of 'over-removal' of content stored by them at the request of users of their platforms in so far as they also remove legal content." (source: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200096en.pdf).

This opinion should provide guidance to the Commission when drafting the DSA to avoid the risk of over-removal of legitimate content and an out-of-its-time distinction between "passive" and "active" hosts.

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. (5K characters max)

Yes, the prohibition of any general monitoring obligation is one of the cornerstones of a successful internet regulation. General monitoring consists of the indiscriminate verification and control of all the online content or behaviour hosted on intermediaries' systems for an unlimited amount of time and thus requires the mandatory use of technical filtering tools against all users. Such an obligation would have inevitable detrimental effects on the ability of people who have done nothing wrong to freely share and access content online. Requiring intermediaries to actively look for potentially illegal content with the aim of removal also implies that platform operators should have the ability and incentive to

properly assess whether any given piece of content is actually illegal under EU law or any of the 27 member state laws. Practice and common sense shows that they have neither and would be pretty bad replacements for our ordinary and criminal courts.

7. Do you see any other points where an upgrade may be needed for the liability regime of digital services acting as intermediaries? (5K characters max)

No

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

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

Consumers have sufficient choices and alternatives to the offerings of online platforms:

Fully disagree

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").

Fully disagree

It is easy for individuals to port their data in an useful form for alternative service providers outside of an online platform.

Fully disagree

There is sufficient level of interoperability between services of different online platform companies.

Fully disagree

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.

Fully agree

It is easy for innovative SME online platforms to expand or enter the market.

Fully disagree

Traditional businesses are increasingly dependent on a limited number of very large online platforms.

Fully agree

There are imbalances in the bargaining power between these online platforms and their business users.

Fully agree

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.

Fully agree

Certain large online platform companies create barriers to entry and expansion in the Single Market (gatekeepers).

Fully agree

Large online platforms often leverage their assets from their primary activities (customer base, data, technological solutions, skills, financial capital) to expand into other activities.

Fully agree

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.

Fully agree

Main features of gatekeeper online platform companies and main relevant criteria for assessing their economic power

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):

5 Large user base

4 Wide geographic coverage in the EU

3 They capture a large share of total revenue of the market you are active/of a sector

4 Impact on a certain sector

5 They build on and exploit strong network effects

3 They leverage their assets for entering new areas of activity

5 They raise barriers to entry for competitors

5 They accumulate valuable and diverse data and information

4 There are very few, if any, alternative services available on the market

5 Lock-in of users/consumers

Other

2. If you replied "other", please list (3K characters max)

3. Please explain your answer. How could different criteria be combined to accurately identify large online platform companies with gatekeeper role? (3K characters max)

We make the distinction between relevant and dominant platforms. By dominant platforms, we understand online or social media platforms that have significant market power in a majority of countries in the EEA and a global revenue above a certain threshold. By relevant platforms, we

understand online or social media platforms that have significant market power in a country within the EEA and a global revenue above a certain threshold.

To give examples, a relevant platform would be a national newspaper with a frequently used reader comment section. A dominant platform would be YouTube or Facebook. For more definitions see: https://www.platformregulation.eu/#definitions-and-basic-concepts

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 strengthen the gatekeeper role:

x 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

consumer reviews on large online platforms

network and/or data infrastructure/cloud services

x digital identity services

x payment services (or other financial services)

physical logistics such as product fulfilment services

data management platforms

x online advertising intermediation services

other. Please specify in the text box below.

Question 5: no epicenter.works response.

Emerging issues

Questions 1-7: no epicenter.works response

9. Are there specific issues and unfair practices you perceive on large online platform companies? (5K characters max)

1. Apple artificially prevents the installation of alternative software sources on its smartphones and tablets running iOS. Thereby, the company uses its market power as a device and operating system maker to control which software users can run on their own devices.

2. Alphabet contractually obliges smartphone makers to install the complete suite of proprietary Google apps (Gmail, Maps, Search, Play Services, etc.) if they wish to gain access to the Google app store ('Play Store'), and prohibits the pre-installation of any competing apps (including competing app stores). Thereby, Alphabet uses its market power in operating systems to push its other services onto people's phones and prevents any competitor to gain a foothold in the market.

3. Facebook obliges users to consent to incredibly intrusive personal data collection and analysis in order to use its services. The company also obliges users to consent to Facebook combining all their personal data from different Facebook-owned services like WhatsApp and Instagram as well as from across the web into one single profile that's then marketed to advertisers. Facebook thereby uses its dominant position as social network to cement its market power in the data and online advertising business.

4. Facebook makes it impossible for competing social networks to enable their users to interconnect with friends on Facebook. Thereby, the company abuses its market power and strong network effects to lock-in its users, to artificially prevent them from getting in touch with 'the outside world', and to suppress any potential competing social network from ever gaining a foothold in that market—most users are already taken by Facebook.

10. In your view, what practices related to the use and sharing of data in the platforms' environment are raising particular challenges? (5K characters max)

1. Regarding user data, a particular challenge is the use of personal data for the purpose of micro-targeted advertising and other content. Micro-targeting online content (the very business model of companies such as Google and Facebook) makes a functioning public debate about the issues discussed online impossible because nobody knows what kind of online content everybody else has been fed. That is why the DSA should limit the micro-targeting of online content on platforms.

At a minimum, most of the current ways of receiving "consent" (through cookie walls) need to be put in line with data protection and privacy legislation. Where consent mechanisms fail to respect the legislation, there must be strong enforcement and redress. If enforcement were to happen as foreseen by existing data protection and privacy legislation, this would mean that personal data could therefore not be used for advertising purposes without the knowledge and informed and explicit consent of the user.

By restricting the way targeted advertising and algorithmic recommendations currently work, companies would lose the incentive to collect personal data in the first place. Such limitations would remove the financial incentives to spread extreme or controversial harmful speech, disinformation and to manipulate elections and democratic processes. There would be less or no invasive cookies (same thing for the banner pop-ups asking you for "consent"), and no more second thoughts about sharing our intimate life with third parties when surfing the web. Finally, if personal data can no longer be accessed by or shared to any third party, it would eliminate the incentive for trafficking data and would force companies to rethink their business models.

Furthermore, the DSA could prohibit advertisers to target users with content based on very sensitive personal data, such as their specific psychological profiles, political opinions, sexual orientations,health status, or any other sensitive personal data. This limitation should include all types of content, no

matter if it is political, issue-based, commercial, or otherwise. This would not impede these of online advertising: publishers, bloggers, app developers, and others can still use generic or context-sensitive online ads in order to generate revenue without collecting any personal data about users.

2. Regarding aggregated statistical information about how large platforms are moderating and curating online content, a particular challenge is the lack of transparency. Today, no one really knows, how many pieces of content Facebook has identified as potentially illegal. Or how many instances of content removal by Twitter have been contested by users. That is why the DSA should introduce the mandatory publication of such data for all large platform operators in a machine-readable pre-defined format. Only then will we be able, as a society, to truly understand the extent to which online platforms contribute to and influence our public debates, how they potentially manipulate people's thinking and pre-determine what individuals read or do not read online. This should also include:

- In how many cases were contested removals reversed?
- How many cases of flagging have been identified as wrongful by platforms and therefore been discarded?
- How many staff do platforms employ to moderate content and in which languages and countries?
- According to which factors do platforms amplify or demote certain content?
- Which categories of personal data can customers use to micro-target platform users with ads or other, non-ad content?
- Who are those customers and how much do they spend on micro-targeting platforms users with what kind of content?

3. We do not believe that the dominance of U.S.-based incumbent platforms and applications can be broken by forcing them to share personal user data with competitors—this would also likely be illegal under the GDPR (this may be different for non-personal data like maps data or industrial information). The reason why today's big tech firms have been able to offer successful digital services is not necessarily because access to lots of personal data is a prerequisite for building world-class digital services. It is rather because through online advertising and the sales of personal data they have amassed such enormous financial resources that they could hire the best people and throw large amounts of money at building and perfecting those services. Being a privacy nightmare is not a prerequisite for building a successful search engine, email app or maps service.

11. What impact would the identified unfair practices can have on innovation, competition and consumer choice in the single market? (3K characters max)

Example 1: Consumers cannot choose to install the best software or the software they like. They are dependent on Apple approving the respective app for its app store. The company has used this power in the past to ban certain types of apps in certain countries (VPN apps in China, HKmaps app in Hong Kong, for example), and to ban all competing browser engines from its devices. As a result, all non-Apple browsers—like Mozilla Firefox, Google Chrome, and Brave—are forced to use Apple's own browser engine WebKit. But Apple could also use this power to slow down or prevent the publication of other apps that compete with its own services, like music streaming or messaging apps.

Example 2: Alphabet's behaviour hurts competition by foreclosing the smartphone app market to any other providers of similar apps/services. As a result, it becomes very hard—if not impossible—for competitors to have their search engines (like Qwant, Duckduckgo, Ecosia), email apps (like FairEmail, Outlook, Protonmail, Tutanota), maps apps (like Maps.me, OSMand), or voice assistants(like Cortana, Alexa, Siri) pre-installed on smartphones running Android. This of course also severely limits user choice.

Example 3: Facebook's combining of personal data without user choice has an immense negative impact on consumer privacy rights. The more companies and digital services that Facebook buys and operates, the harder it will be for people to use services without being forced to give up their personal data to Facebook. The situation is aggravated by the inclusion of Facebook tracking code into many major websites (such as the "Like" button). This code channels personal data to Facebook whenever someone visits a website, regardless of whether that person has a Facebook account or not.

Example 4: Facebook maintains several APIs that allow developers to interoperate with its core product. However, for developers to be able to access such APIs, it is necessary to agree to Facebook's platform policy, which prevents developers from offering apps that "offer experiences that change" Facebook, and to respect the "limits we've placed on Facebook functionality". Thus, Facebook deliberately refuses to allow competitors to interconnect or interoperate and prevents them from overcoming the network effects that cement Facebook's dominant position as a social network. If users were enabled to move their online lives to alternative networks without losing their connections on the dominant Facebook platform, a whole market would be liberated. Even new markets could be created by allowing startups to develop services on top of Facebook that interoperate with the platform. This would empower users to take advantage of additional functionalities and services (like a content moderation add-on or a better way to show and filter the Facebook timeline).

Question 12: no epicenter.works response.

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? (3K characters max)

The gatekeeper role of large online platform companies has mostly negative societal and economic effects:

- By reducing the diversity of online platforms, the gatekeeper prevents fair competition nohow to best deal with illegal content or how to best protect users against harm. As a result, it is not only users but also regulators and legislators who depend on one single private company to come up with viable solutions rather than being able to choose from the best ideas in the market. In a gatekeeper scenario, regulators and legislators also have no choice but to trust the gatekeeper when they claim there are no better solutions than theirs.
- For social networks, the gatekeeper role centralises an immense power over what people see and read, and what publishers can successfully distribute online. A social network's content curation algorithm can decide how many readers a journalistic work will reach and which leaked documents are being censored (see the example of #BlueLeaks suppressed by Twitter). Usually those algorithms are neither transparent nor verifiable. Add to this, that advertising-

funded companies like Youtube or Facebook don't even attempt to provide fair or balanced content curation; instead they promote and demote content depending on what makes people stick to their screens: scandal, outrage, hate, social division. This unhealthy dependence on a single, centrally-controlled 'information bottleneck' is at least partly responsible for the difficult situation press publishers are in today.

- Gatekeepers often also stifle innovation and prevent the success of new entrants. For example, Facebook acts as gatekeeper to 2.5+ billion social network users. Multi-homing in social networks does not seem to be possible, so the only way to reach those users with similar functionality would be to be interoperable with Facebook. But that's something the company actively prevents to protect their gatekeeper role. The same can be said of Apple,which—by prohibiting alternative software sources on iOS devices—uses its gatekeeper position as the only operating system provider for Apple devices to prevent competing app stores (and thereby potentially competing apps) to enter the market on iOS app stores.

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. (3K characters max)

Many classical media outlets offer significant parts of their content on platforms like Facebook or YouTube. Often these outlets are even public broadcasters that finance their content with tax payer money. By publishing their content on these commercial platforms they often consent to a license that allows for the commercial exploitation of this content. A free license like Creative Commons would enable other platforms like Wikipedia or educational platforms to also re-use and re-contextualise this content for greater societal benefit.

Regulation of large online platform companies acting as gatekeepers

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

I agree to a certain extent

I disagree to a certain extent

I disagree

I don't know

2. Please explain (3K characters max).

The DSA should put in place rules, such as mandatory interoperability, that are able to limit the gatekeeper role that large online platform companies have acquired, as well as the resulting negative effects. Such rules need to be specific to these gatekeepers as they would otherwise risk hurting smaller players trying to compete with them. As a result, the goal of increased user choice and

freedom would not be achieved. Interoperability mandates would also breathe life into the data portability right introduced by the GDPR that has been of little use so far because of a lack of spaces where users could port their data to. Currently, it is unclear what personal data users are able to port and under which circumstances. Thus, the DSA should also clarify the GDPR's data portability right.

Interoperability mandates should be accompanied by strong privacy, security and non-discrimination rules. To avoid the abuse of interoperability, and data made available through interoperability, this data should not be available for general commercial use. Therefore, any data made available for the purpose of interoperability should only be used for maintaining interoperability, safeguarding user privacy, and ensuring data security. Users must be in full control of how, when and for what purposes their personal data is shared. The principles underpinning the GDPR and other relevant legislation,such as data-minimisation and privacy by design and default must be protected.

Interoperability measures must not compromise users' security or be construed as a reason that prevents platforms from taking efforts to keep users safe. When intermediaries do have to suspend interoperability to deal with security issues, they should not exploit such situations but rather communicate transparently, resolve the problem, and reinstate interoperability interfaces within a reasonable and clearly defined time frame.

Access to interoperability interfaces should not discriminate between different competitors and should not demand strenuous obligations or content restrictions. Interoperability interfaces, such as APIs, must also be easy to find, well-documented, and transparent.

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

No

I don't know

4. Please explain your reply and, if possible, detail the types of prohibitions that should in your view be part of the regulatory toolbox. (3K characters max)

Gatekeepers should be prohibited to build digital silos / walled gardens. They should be obliged by law to allow competing services to interoperate with the ecosystem they are gatekeeping and freely build services on top of or compatible with the one that the gatekeeper controls.

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

***** Yes

No

I don't know

6. Please explain your reply and, if possible, detail the types of obligations that should in your view be part of the regulatory toolbox. (3K characters max)

Gatekeepers should be prohibited to build digital silos / walled gardens. They should be obliged by law to allow competing services to interoperate with the ecosystem they are gatekeeping and freely build services on top of or compatible with the one that the gatekeeper controls. They should also enable users to delegate specific tasks or elements of their online experiences (i.e. content moderation) to appropriate third parties.

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

No

I don't know

8. Please explain your reply. (3K characters max)

New legal obligations for gatekeepers (and other intermediaries) are only going to have their intended impact if they can be reliably enforced. The example of GDPR has shown that enforcement is crucial in the pursuit of justice and comparable compliance standards across all EU member states.

An independent European regulatory authority should therefore be tasked to oversee compliance with these obligations. The regulator should be tasked with monitoring and enforcing compliance,issuing fines, auditing intermediaries covered by the DSA, as well as receiving complaints from affected individuals and organisations. It must be equipped with enough resources to effectively control and enforce the obligations for gatekeepers and all other entities covered by the DSA and should have proven experience in the field of internet regulation, the platform economy and fundamental rights. The independent regulator should not, however, be empowered to take content moderation or content decisions, as such decisions should ultimately be in the hands of the independent judiciary or national regulators for a first instance of arbitration body.

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

No

I don't know

10. If yes, please explain your reply and, if possible, detail the types of case by case remedies. (3K characters max)

Specific regulatory intervention is necessary to address competition, consumer protection and fundamental rights issues without delay. The digital market moves rapidly and therefore people and companies affected by the abuse of a gatekeeper position cannot wait until antitrust authorities have spent years to analyse and formulate theories of harm. The functioning and effects of the abuse of a gatekeeper position are sufficiently well studied to enable a regulator to step in and impose immediate remedies.

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

No

12. Please explain your reply (3K characters max)

This task could be taken on either by the regulator described in our answer to questions 7 and 8 or by DG COMP.

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. (3K characters max)

This task could be taken on either by the regulator described in our answer to questions 7 and 8 or by DG COMP.

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

At national level

***** At EU level

Both at EU and national level.

I don't know

Question 15: no epicenter.works response.

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. (3K characters max)

Yes, both perspectives can be taken into consideration. In this case, the DSA must however clearly specify the objectives that a regulator is allowed to pursue. Concretely, the regulator should not be able to impose remedies on a gatekeeper vaguely citing some “negative societal effects”. The DSA

should include a concrete list of such effects that would empower the regulator to act. This is crucial for protecting legal certainty for companies and for limiting the powers of the regulator to what is necessary and appropriate.

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? (3K characters max)

The DSA should oblige gatekeeper platforms to open up their digital silos and provide meaningful options to allow users to 'port' their data to other platforms. Besides enabling the right to data portability contained in the GDPR, users should also be able to interconnect with people across competing platforms. This would enable new market entrants and competitors to compete on the merits of their services (like content moderation, user interface, privacy, features, business model,etc.).

Interoperability mandates should be accompanied by strong privacy, security and non-discrimination rules. To avoid the abuse of interoperability, and data made available through interoperability, this data should not be available for general commercial use. Therefore, any data made available for the purpose of interoperability should only be used for maintaining interoperability, safeguarding user privacy, and ensuring data security. Users must be in full control of how, when and for what purposes their personal data is shared. The principles underpinning the GDPR and other relevant legislation,such as data-minimisation and privacy by design and default must be protected.

Interoperability measures must not compromise users' security or be construed as a reason preventing platforms from taking efforts to keep users safe. When intermediaries do have to suspend interoperability to deal with security issues, they should not exploit such situations to break interoperability but rather communicate transparently, resolve the problem, and reinstate interoperability interfaces within a reasonable and clearly defined time frame.

Access to interoperability interfaces should not discriminate between different competitors and should not demand strenuous obligations or content restrictions. Interoperability interfaces, such as APIs, must also be easy to find, well-documented, and transparent.

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? (3K characters max)

See answer to question III.emerging issues.14.

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

Swift and effective cross-border cooperation and assistance across Member States

* Capacity building within Member States

* High level of technical capabilities including data processing, auditing capacities

Cooperation with extra-EU jurisdictions

* Other

20. If other, please specify (3K characters max)

The regulator should be equipped with enough resources to effectively control and enforce the obligations for intermediaries under the DSA and its staff must have proven experience in the field of internet regulation, the platform economy and fundamental rights.

Question 21: no epicenter.works response.

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

* Monitoring powers for the public authority (such as regular reporting)

* Investigative powers for the public authority

* Other

23. Other – please list (3K characters max)

The regulator has to ex-ante approve the Terms of Service of any dominant social media platform (including other documents relevant to content moderation and account suspension, like Community Guidelines and Code of Conducts). See: https://www.platformregulation.eu/#recommended-enforcement-via-european-platform-regulator

Question 24: no epicenter.works response.

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 Current competition rules are enough to address issues raised in digital markets

4 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

4 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

5 There is a need for a New Competition Tool allowing to 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.

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. (3K characters max)

In order to limit the damage that the abuse of a gatekeeper position in online platform markets can do, DG COMP or a similar regulator should have the power to use a New Competition Tool in order to address structural risks and a lack of competition. In addition, the DSA should provide a regulatory framework to act on a case-by-case basis if there is evidence that a gatekeeper has negative effects on competition.

Question 27: no epicenter.works response.

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?

Yes, always

Sometimes: but I can find the information when this is not immediately clear

* Sometimes: but I cannot always find this information

I don't know

No

Questions 2-14: no epicenter.works response.

15. From your perspective, what measures would lead to meaningful transparency in the ad placement process? (3K characters max)

Together with EDRi, we call for the implementation of strong privacy and data protection rules, transparency and a legally binding, human-rights based approach. Paired with meaningful enforcement, this will ensure that the online advertising industry can be held accountable for the way it shapes our online environment. Regarding ad placement, understanding the way in which Real Time

Bidding (RTB) works and how ads are allocated is essential for policy-making regarding this type of platform.

As a first step the DSA should require transparency for users about how ads are targeted at them and implement mandatory human rights impact assessments and reporting via ad archive APIs (seethe section "so what should companies do" at https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/so-what-should-companies-do) about how algorithms place ads (see https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like). On Human Rights Impact Assessments for AI, please see EDRi member Access Now's report 'Trust and excellence — the EU is missing the mark again on AI and human rights' here: https://www.accessnow.org/trust-and-excellence-the-eu-is-missing-the-mark-again-on-ai-and-human-rights.

None of this however should lift the burden of ad-tech operators from meeting the requirements for consent under the GDPR, since other bases for processing have been ruled out by DPAs.

In view of the above, we suggest that binding transparency requirements must be put in place, including

- Complete, centralised and public ad archives (see Part III of EDRi member Panoptykon's recommendations of "Who (really) targets you? Facebook in Polish election campaigns", at https://panoptykon.org/political-ads-report and our proposal at https://www.platformregulation.eu/#must-advertisement-archive
- Fully functional and effective ad archive APIs for researchers (see https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like). Problems on the lack of access to APIs for researchers have been discussed by AlgorithmWatch here: https://algorithmwatch.org/en/story/left-on-read-facebook-data-access.

In addition to this, we advocate for a strong enforcement of the General Data Protection Regulation (GDPR) and the adoption of an equally strong ePrivacy Regulation that eliminates the current abusive design of tracking advertising: RTB, cookie synchronisation, first-party tracking, use of cookie walls, ensuring that consent is properly obtained and that privacy by design and by default becomes baked into the online advertising industry.

Finally, the promotion of tracking-free ad business models (like the one at NPO: https://brave.com/npo) and further research are essential steps in the right direction. Similar actions to protect readers' privacy have been launched by the New York Times (see https://open.nytimes.com/how-the-new-york-times-thinks-about-your-privacy-bc07d2171531).

16. What information about ads displayed online should be made publicly available? (3K characters max)

It is highly problematic that platform companies do not provide the public with complete information about why they are targeted with ads in general, and particularly "political" ads. Facebook, Google, and Twitter, must provide the same quality of information about why users are seeing an ad as advertisers are able to target users on these platforms.

According to EDRi member Privacy International, this information should include at least: 1) the source of the data used to target ads, 2) the target audience of the advertiser and actual audience of the

advertiser, 3) information about if the ad was micro-targeted (see https://www.privacyinternational.org/explainer/3288/why-advertising-transparency-important).

Furthermore, we suggest following Mozilla's suggestions on how to build an effective ad archive API(see https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-likeand check for potential pitfalls here: P. Leerssen, J. Ausloos, B. Zarouali, N. Helberger, C. H. de Vreese, Platform ad archives: promises and pitfalls, October 2019, available at: https://policyreview.info/articles/analysis/platform-ad-archives-promises-and-pitfalls).

Mandatory ad libraries should at least include:

- information about the content of the advert itself, including an advert category and an advert description;
- detailed targeting criteria and options selected by advertisers (including the data source,lookalike/custom audiences, A/B testing used, optimisation goal);
- information about its impact (aggregated information about the types of people who actually saw the advert);
- a general, user-friendly explanation of optimisation algorithms used by the platform in the process of targeting ads (including the objective of the algorithm and explanation of the logic of optimisation); and
- an obligation to conduct and publish human rights impact assessments for algorithms used for targeting ads.

17. Based on your expertise, which effective and proportionate auditing systems could bring meaningful accountability in the ad placement system? (3K characters max)

Any auditing system must include an obligation for platforms to produce thorough documentation of their algorithms used for ad targeting, including fairness criteria for their ad optimisation process, in particular the obligation to conduct and publish Human Rights Impact Assessments. For details about such Impact Assessments and auditing mechanisms please see EDRi member Panoptykon's AI position paper:

https://panoptykon.org/sites/default/files/stanowiska/panoptykon_ai_whitepaper_submission_10.06.2010_final.pdf.

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? (3K characters max)

As Paddy Leerssen LL.M., PhD candidate at the Institute for Information Law (IviR) of the University of Amsterdam noted, the difficulty of defining what a political ad is: "If you focus only on official election ads, then a lot of important political activity is ignored. For instance, many of the Russian ads disseminated on Facebook during the 2016 U.S. election agitated on polarizing social issues without directly referencing the election. To capture such activity, a broader definition of political issues is needed — but this is complex and subjective. Is the coronavirus political, for instance?What about Bitcoin? Or climate change?" Similarly, Ranking Digital Rights stated that "[p]latforms should not

differentiate between commercial, political, and issue ads, for the simple reason that drawing such lines fairly, consistently, and at a global scale is impossible and complicates the issue of targeting."

Although it is quite difficult to define political advertising, if we had to we would use the definition collected by Borgesius et al., where political micro-targeting is a technique that "involves creating finely honed messages targeted at narrow categories of voters' based on data analysis garnered from individuals' demographic characteristics and consumer and lifestyle habits. Online political micro-targeting can take the "form of political direct marketing in which political actors target personalised messages to individual voters by applying predictive modelling techniques to massive troves of voter data" (...) "Online political micro-targeting is used, for example, to identify voters who are likely to vote for a specific party and therefore can be targeted with mobilising messages. (For ease of reading, we also refer to 'micro-targeting'). Micro-targeting also enables a political party to select policy stances that match the interests of the targeted voter – for instance family aid for families, or student benefits for students" (see https://ssrn.com/abstract=3128787).

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? (3K characters max)

For political advertisement it is vital that the user is also displayed the entity that has paid for this advertisement. At best, the advertisement archive should retain political advertisements for a longer period and also oblige the platform to make the sponsor public with a follow the money aproach.

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? (3K characters max)

Enhanced transparency and accountability, in addition to a strong ePrivacy Regulation (when finally adopted) and stronger GDPR enforcement, will undoubtedly redefine the way online advertising works. Much of the current online tracking based advertising will need to find the adequate legal basis or change their practices and some are starting to do so.

For example public broadcasters such as NPO (see https://brave.com/npo) are already providing very successful alternatives to the current invasive business models which can be applied to most of the other public and private publishers and broadcasters. Through this change, NPO have be enable to even increase (see https://www.openrightsgroup.org/blog/is-ethical-ad-tech-possible) their advertising profits after deciding not to track the people accessing their services, even during the COVID pandemic where most advertising revenues were going down.

By redefining the way advertising works (like banning tracking by design and by default practices) the power of the duopoly of advertising intermediaries that Google and Facebook represent at the moment will be reduced. For this to happen, EU legislation should introduce systemic changes and promote the return to context-based advertising (in the ad placing system). It should promote human-centric content curation systems where people will only be targeted if they control what kind of content they are going to see and interact with. This would put publishers and readers in charge and

revert the current practices where advertising companies profile every single person in order to target them with content and ads based on their current and predicted future behaviour.

21. Are there other emerging issues in the space of online advertising you would like to flag? (3K characters max)

- The GDPR must be enforced to ensure that the right to data protection is prioritised over advertising business models. For this to happen, member states must give DPAs the financial resources to investigate infringements (see response of the ICO on why it fails to investigate: https://twitter.com/johnnyryan/status/1258381720061124608).
- A strong and clear ePrivacy Regulation must urgently enter into force and be implemented effectively.
- Industry standards and frameworks must not permit the exploitative and intrusive use of personal data at the core of the advertising business model of most platforms.
- GDPR requires data protection by design and by default. Privacy should therefore be embedded at all levels. Instead of tracking users by default and requiring them to opt out, any tracking ads should be on a strict opt-in basis.
- Advertising-based platform companies must be compelled to uphold fundamental rights standards in the creation, development and use of algorithms across all EU regulations. This includes AI, platform regulation, data protection, among others. Furthermore, Recommendation CM/Rec(2020) of the Council of Europe (https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154) regarding the human rights impact of algorithmic systems must be respected.
- To escape current monopolies it is key that users can move between similar services without being cornered in centralised silos. This requires opening up dominant platforms via secure APIs, enabling users to move to alternative platforms without losing their contacts (see EDRi's DSA position paper at https://edri.org/wp-content/uploads/2020/04/DSA_EDRiPositionPaper.pdf and https://edri.org/the-impact-of-competition-law-on-your-digital-rights and https://www.eff.org/deeplinks/2019/10/adversarial-interoperability.
- Binding transparency requirements must be put in place, including: (a)fully functional and effective ad archive APIs for researchers (see https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-likeandhttps://algorithmwatch.org/en/story/left-on-read-facebook-data-access); and (b) more details on recommendations linked to political advertising, see https://panoptykon.org/political-ads-report.
- Recommendation and content moderation algorithms must be audited (see https://arxiv.org/pdf/2001.10581.pdf). Online advertising companies and platforms using their services for advertising purposes should be transparent about the use and any practical impact of the automated tools they use.

Questions on smart contracts, the situation of self-employed individuals, and reinforcing the Single Market: no epicenter.works response.

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

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? (5K characters max)

From our perspective the cooperation between regulatory authorities within the Single Market exhibits many problems in practice. In the field of telecoms regulation, we have observed divergent interpretations of the Open Internet regulation and drastically different approaches to enforcing the same regulation between different member states. BEREC mostly works as a forum for expert discussion on the working level. In order to address enforcement deficits in particular member states, other regulatory agencies can only resort to soft power. For example, only extended pressure by peers lead the Portuguese telecoms regulator ANACOM to act in the case of an internet access product called "Smart Net" from the incumbent operator MEO that combined technical discrimination with low general purpose data volume. (https://en.epicenter.works/content/civil-society-urges-portuguese-telecom-regulator-to-uphold-net-neutrality)

Similarly, for multiple years the Irish telecoms regulator COMREG released annual reports in which it listed all the enforcement actions that would be required to ensure net neutrality in Ireland, but then ended with explaining that the Irish legislator had not transposed the regulation and that therefore COMREG was unable to take enforcement action. In comparison, the Austrian telecoms regulator RTR had to operate in a similar situation for over one and a half years, yet the RTR still enforced the Open Interner Regulation vigorously and justified its mandate with the primacy of EU law. (https://www.comreg.ie/media/dlm_uploads/2017/06/ComReg-1761.pdf and https://www.comreg.ie/publication/implementation-of-eu-net-neutrality-regulations-in-ireland-2018)

Sadly, the enforcement of the GDPR is another example for where enforcement throughout the Single Market is severely lacking. Over two years after the Regulation came into effect, the Irish data protection authority has yet to take any decisive enforcement action in many important cases (https://noyb.eu/en/open-letter). The EDPB has not established itself as a mechanism to prevent exactly these kinds of enforcement bottlenecks that allow digital service providers to operate potentially unlawful business models throughout the Single Market.

Lastly, we would like to stress that cooperation between different regulators is also often unsatisfactory. For example, the Open Internet Regulation explicitly mandates the compatibility with existing data protection law of traffic management measures that process personal data. Yet, while the use of Deep Packet Inspection technology in internet access products that make use of traffic management is increasing, which is highly questionable in view of Union law such as the ePrivacy Directive, BEREC only contacted the EDPB for an opinion on the lawfulness of the use of such technologies after public pressure from civil society and on the occasion of the reform of its guidelines implementing the Regulation. (https://edri.org/ngos-and-academics-warn-against-deep-packet-

inspection/) The mere possibility of cooperation between different regulators does not necessarily mean that it is made use of.

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 Clearly assigned competent national authorities or bodies as established by Member States for supervising the systems put in place by online platforms

1 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.)

3 Cooperation mechanism with swift procedures and assistance across national competent authorities across Member States

3 Coordination and technical assistance at EU level

5 An EU-level authority

1 Cooperation schemes with third parties such as civil society organisations and academics for specific inquiries and oversight

5 Other: please specify in the text box below

3. Please explain (5K characters max)

A strong central EU platform regulator is the only effective enforcement mechanism for procedural and structural rules in the DSA. Other models placing the primary enforcement burden on national authorities with various forms of cooperation between regulators and member states has proved unsatisfactory with regard to previous digital rights legislation. A platform regulator should be established as an EU agency, analogously adhering to the Common Approach. This would ensure strong transparency and conflict of interest policies, which are sometimes lacking on the national level.

It is important to stress that this EU platform regulator should not be in charge of redress in individual disputes regarding content moderation decisions. These questions require cultural and linguistic context to resolve and should not be handled by a central authority. National authorities (media regulators) can be in charge of these processes. Instead, the platform regulator should handle questions that relate to the platform as a whole. Media and data protection authorities should be able to trigger proceedings with the EU platform regulator but the platform regulator should be in charge of the procedure.

4. What information should competent authorities make publicly available about their supervisory and enforcement activity? (3K characters max)

Competent authorities should publish regular transparency reports about the activities they have undertaken to fulfil their mandate. They should be inclusive in their working methods and include a wide variety of stakeholders in the creation of guidelines that detail specific aspects of their work. The employees of the agency should engage in public speaking at conferences and give interviews to inform the public about their work.

5. What capabilities – type of internal expertise, resources etc. - are needed within competent authorities, in order to effectively supervise online platforms? (3K characters max)

This agency requires staff with expertise and experience in legal, IT (and in particular, reverse engineering), mathematics and economics. The organisation needs to be independent and impartial in order to accomplish its mission. This includes the necessity to sufficiently finance the organisation. One way to achieve this is to have regulated market participants above a certain size to which the DSA applies contribute to its budget in proportion to their size. (This model has worked well for the Austrian telecoms and media regulators.)

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?

x Yes, if they intermediate a certain volume of content, goods and services provided in the EU

x Yes, if they have a significant number of users in the EU

No

x Other

I don't know

Question 7: Please explain

Both services that intermediate a certain volume of content, goods and services provided in the EU or have a significant number of users in the EU should be subject to such supervision.

Question 8: no epicenter.works response.

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? (3K characters max)

See answers to questions 1 and 3. The EDPB model has not proven effective in enforcing the GDPR and should not be used for the DSA.

Question 10: no epicenter.works response.

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. (3K characters max)

In the revised AVMS Directive 2018, Article 30b provides the legal ground for ERGA, establishing it and listing its composition and tasks that include: to advise and assist the Commission, to cooperate and exchange information, and to give opinions when requested by the Commission. ERGA is thus granted procedural autonomy. However, it remains to be seen how the cross-border mechanism as well as ERGA's role will be implemented and enforced, as Member States have time to implement the Directive until 19 September 2020. Therefore, it would be rather premature to present ERGA as the right model for future DSA oversight.

While Article 30 requires adequate financial and human resources for regulators, as well as enforcement powers, allowing them to carry out their functions effectively and to contribute to the work of ERGA, it does not seem to reflect the reality on the ground. Many regulatory authorities face challenges regarding funding and human resources and have raised concerns over a lack of human resources necessary for effective handling of their tasks. That did not prevent some national legislators in the EU from placing even more enforcement and oversight functions for national content governance legal frameworks to their competence. Furthermore, ERGA is currently not equipped to monitor the independence of media regulators.

Questions 12-14: no epicenter.works response.