

---

European Commission Consultation on the  
**Digital Services Act Package**

# OPEN SOCIETY EUROPEAN POLICY INSTITUTE'S RESPONSE

Authors:  
Guillermo Beltrà  
Pamela Valenti

September 2020

**OPEN SOCIETY  
EUROPEAN POLICY  
INSTITUTE**

---

---

The Open Society European Policy Institute is the EU policy and advocacy branch of the Open Society Foundations network, based in Brussels. It works to influence and inform decision-making on EU laws, policy, funding, and external action to maintain and promote open societies in Europe and beyond.

In February 2020, the European Commission published the [“European Digital Strategy: Shaping Europe’s Digital Future”](#), an ambitious political roadmap outlining its vision to modernise Europe’s rules governing digital markets and online platforms.

The planned Digital Services Act package announced in February and scheduled to be published in December 2020 is set to become a regulatory overhaul of how the EU regulates the digital world. It should contain two main pillars:

- New and revised rules to deepen the Single Market for Digital Services, by updating the e-Commerce Directive to harmonise the responsibilities of online platforms and information service providers and reinforce the oversight over platforms’ content policies, increase transparency of content moderation systems, and possibly mandate data access requirements and algorithmic audits.
- New rules to ensure that markets dominated by so-called ‘digital gatekeepers’, or very large platforms with an unchecked power over vertical or adjacent markets and benefitting from strong network effects, remain fair and contestable for innovators, businesses, and new market entrants.

To prepare these ambitious legislative initiatives, the European Commission launched a series of public consultations to gather stakeholders’ views. In September 2020, Open Society European Policy Institute submitted its response to the public consultation. Open Society European Policy Institute’s submission, developed in collaboration with other Open Society Foundations programmes, provides recommendations for ambitious EU action in the areas of competition in digital markets, content governance and the protection of fundamental rights, in particular of freedom of expression, countering disinformation, and guaranteeing an efficient oversight and enforcement architecture.

For more information, please contact:

Guillermo Beltrà, [guillermo.beltra@opensocietyfoundations.org](mailto:guillermo.beltra@opensocietyfoundations.org)

Pamela Valenti, [pamela.valenti@opensocietyfoundations.org](mailto:pamela.valenti@opensocietyfoundations.org)

## **OPEN SOCIETY FOUNDATIONS**

© 2020 Open Society Foundations



This publication is available as a PDF on the Open Society Foundations website under a Creative Commons license that allows copying and distributing the publication, only in its entirety, as long as it is attributed to the Open Society Foundations and used for noncommercial educational or public policy purposes. Photographs may not be used separately from the publication.

[opensocietyfoundations.org](https://opensocietyfoundations.org)

---

The Commission is initiating the present open public consultation as part of its evidence gathering exercise, in order to identify issues that may require intervention through the Digital Services Act, as well as additional topics related to the environment of digital services and online platforms, which will be further analysed in view of possible upcoming initiatives, should the issues identified require a regulatory intervention.

The consultation contains 6 modules (you can respond to as many as you like):

1. How to effectively keep users safer online?
2. Reviewing the liability regime of digital services acting as intermediaries?
3. What issues derive from the gatekeeper power of digital platforms?
4. Other emerging issues and opportunities, including online advertising and smart contracts
5. How to address challenges around the situation of self-employed individuals
6. offering services through online platforms?
7. What governance for reinforcing the Single Market for digital services?

### **Digital services and other terms used in the questionnaire**

The questionnaire refers to (or 'information society services', **digital services** within the meaning of the E-Commerce Directive), as 'services provided through electronic means, at a distance, at the request of the user'. It also refers more narrowly to a subset of digital services here termed **online intermediary services**. By this we mean services such as internet access providers, cloud services, online platforms, messaging services, etc., i.e. services that generally transport or intermediate content, goods or services made available by third parties.

Parts of the questionnaire specifically focus on online platforms – such as e-commerce marketplaces, search engines, app stores, online travel and accommodation platforms or mobility platforms and other collaborative economy platforms, etc.

Other terms and other technical concepts are explained in a glossary.

# I. HOW TO EFFECTIVELY KEEP USERS SAFER ONLINE?

This module of the questionnaire is structured into several subsections:

**First**, it seeks evidence, experience, and data from the perspective of different stakeholders regarding illegal activities online, as defined by national and EU law. This includes the availability online of illegal goods (e.g. dangerous products, counterfeit goods, prohibited and restricted goods, protected wildlife, pet trafficking, illegal medicines, misleading offerings of food supplements), content (e.g. illegal hate speech, child sexual abuse material, content that infringes intellectual property rights), and services, or practices that infringe consumer law (such as scams, misleading advertising, exhortation to purchase made to children) online. It covers all types of illegal activities, both as regards criminal law and civil law.

It then asks you about other activities online that are not necessarily illegal but could cause harm to users, such as the spread of online disinformation or harmful content to minors.

It also seeks facts and informed views on the potential risks of erroneous removal of legitimate content. It also asks you about the transparency and accountability of measures taken by digital services and online platforms in particular in intermediating users' access to their content and enabling oversight by third parties. Respondents might also be interested in related questions in the module of the consultation focusing on online advertising.

**Second**, it explores proportionate and appropriate responsibilities and obligations that could be required from online intermediaries, in particular online platforms, in addressing the set of issues discussed in the first sub-section.

This module does not address the liability regime for online intermediaries, which is further explored in the next module of the consultation.

## MAIN ISSUES AND EXPERIENCES

### Illegal content

**Q1.** Did you ever come across illegal content online (for example illegal incitement to violence, hatred or discrimination on any protected grounds such as race, ethnicity, gender or sexual orientation; child sexual abuse material; terrorist propaganda; defamation; content infringing intellectual property rights, consumer law infringements)?

- No, never
- Yes, once
- Yes, several times
- I don't know

**Q2.** What measure did you take?

- I reported it to the platform via its existing reporting procedure
- I contacted the online platform by other means to report the illegal content
- I contacted a national authority
- I contacted a consumer organisation
- I did not take any action
- I took a different action. Please specify in the text box below

**Q3.** Please specify

**Q4.** How easy was it for you to find information on where you could report the illegal content/activity?

Please rate from 1 star (very dissatisfied) to 5 stars (very satisfied)



**Q5.** How easy was it for you to report the illegal content/activity?

Please rate from 1 star (very dissatisfied) to 5 stars (very satisfied)



**Q6.** How satisfied were you with the procedure following your report?

Please rate from 1 star (very dissatisfied) to 5 stars (very satisfied)



**Q7.** Are you aware of the action taken following your report?

- Yes
- No

## Transparency

**Q8.** If you provided a notice to a digital service asking for the removal or disabling of access to such content or offering of goods or services, were you informed about the follow-up to the request?

- Yes, I was informed
- Yes, but not on every occasion / not by all the platforms
- No, I was never informed
- I don't know

**Q9.** 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.

Response from Open Society European Policy Institute

Too often, poor or no information is provided about how recommendation systems work. Most of the time when information is provided, it is overly general, lacks detail and is not understandable or relatable for users. Sometimes it is easy to see that a product or content has been suggested because of a previous search; but this is not always the case, and not on all platforms. Therefore, enhanced transparency of the algorithmic systems involved in the recommendation of content or products is necessary as a mandatory requirement for all platforms.

Meaningful **transparency** measures on sponsored and recommended content and products should include:

- **Disclosures on why content is shown:** companies should provide more meaningful information on the origin of the content. This should include information on why certain ads are presented to users, and what demographics those ads are targeting. Standards for such disclosures should be mandatory, clear and enforceable.
- **Mandatory ad libraries** for all platforms, based on technical standards to be developed by the European Commission, for the design and functioning of advertisements;
- The creation of **independent auditing bodies** allowing for oversight by national governments and EU institutions of online advertising and targeting criteria.

## **Activities which could cause harm but are not, in themselves, illegal**

**Q10.** In your experience, are children adequately protected online from harmful behaviours, such as grooming and bullying, or inappropriate content?

Response from Open Society European Policy Institute

We support the points raised on this by one of our partner organisations, Worker Info Exchange (<https://workerinfoexchange.org/>):

Rideshare platforms such as Uber do not do enough to enforce their minimum age policy for use. This puts the driver/worker in a difficult position to enforce. In the UK and other countries, drug dealers are known to use minors on services such as Uber to transport drugs.

Also, Deliveroo also ask riders to do age verification for delivery of alcohol and tobacco deliveries. Deliveroo and other similar platforms insist these workers are self-employed; if so, they should not bear responsibility for age verification in this way.

The platform delivery company and /or the vendor should take greater responsibility.

**Q11.** To what extent do you agree with the following statements related to online disinformation?

	FULLY AGREE	SOMEWHAT AGREE	NEITHER AGREE NOT DISAGREE	SOMEWHAT DISAGREE	FULLY DISAGREE	I DON'T KNOW / NO REPLY
1. Online platforms can easily be manipulated by foreign governments or other coordinated groups to spread divisive messages	X					
2. To protect freedom of expression online, diverse voices should be heard	X					
3. Disinformation is spread by manipulating algorithmic processes on online platforms	X					
4. Online platforms can be trusted that their internal practices sufficiently guarantee democratic integrity, pluralism, non-discrimination, tolerance, justice, solidarity and gender equality.					X	

**Q12.** Please explain

Response from Open Society European Policy Institute

Disinformation is a widespread, complex societal problem that requires a multifaceted and consistent response. There is ample evidence that foreign powers as well as European national governments have used disinformation as a weapon to manipulate public discourse and skew the democratic debate. Europe (and the world) faces the immense challenge of addressing this problematic phenomenon while at the same time ensuring that all voices can be heard online.

Addressing the disinformation phenomenon requires different public policies for different stages of the 'disinformation chain': the source of the misleading or incorrect information, the channel through which it transmits, and the recipient of the information.

Online platforms are the most common transmission channels for disinformation, and they have massively benefitted financially from its existence. Many of these platforms operate on a business

model that seeks to grab users' attention and maximise the amount of time users spend on the platforms. Their algorithms therefore often tend to reward polarising and shocking content.

Different self-regulatory initiatives have been tried, and while they may have helped advance the conversation (both between the platforms themselves and with policy-makers), these initiatives have not provided any meaningful solution. A notable example in the EU is the fact that actions by platforms in the context of the EU Code of Practice on Disinformation failed to deliver the promised results and transparency that would have been necessary to adequately assess platforms' efforts to comply with the Code. By focusing on content takedowns, platforms have so far provided insufficient information on critical issues and processes, such as information suppression, content curation and distribution, targeting mechanisms, and ad delivery optimisation.

Strong political action is therefore long overdue to address the disinformation problem in Europe.

For a list of necessary urgent public policy measures, please refer to question 22 in section 2 below.

## CLARIFYING RESPONSIBILITIES FOR ONLINE PLATFORMS AND OTHER DIGITAL SERVICES

**Q13.** What responsibilities should be legally required from online platforms and under what conditions? Should such measures be taken, in your view, by all online platforms, or only by specific ones (e.g. depending on their size, capability, extent of risks of exposure to illegal activities conducted by their users)? If you consider that some measures should only be taken by large online platforms, please identify which would these measures be.

	YES, BY ALL ONLINE PLATFORMS, ACCORDING TO THE ACTIVITIES THEY INTERMEDIATE (E.G. CONTENT HOSTING, SELLING GOODS OR SERVICES)	YES, ONLY BY LARGER ONLINE PLATFORMS	YES, ONLY PLATFORMS AT PARTICULAR RISK OF EXPOSURE TO ILLEGAL ACTIVITIES BY THEIR USERS	SUCH MEASURES SHOULD NOT BE LEGALLY REQUIRED
1. Maintain an effective 'notice and action' system for reporting illegal goods or content	X			
2. Maintain a system for assessing the risk of exposure to illegal goods or content				X
3. Have content moderation teams, appropriately trained and resourced		X		



	YES, BY ALL ONLINE PLATFORMS, ACCORDING TO THE ACTIVITIES THEY INTERMEDIATE (E.G. CONTENT HOSTING, SELLING GOODS OR SERVICES)	YES, ONLY BY LARGER ONLINE PLATFORMS	YES, ONLY PLATFORMS AT PARTICULAR RISK OF EXPOSURE TO ILLEGAL ACTIVITIES BY THEIR USERS	SUCH MEASURES SHOULD NOT BE LEGALLY REQUIRED
4. Systematically respond to requests from law enforcement authorities				X
5. Cooperate with national authorities and law enforcement, in accordance with clear procedures	X			
6. Cooperate with trusted organizations with proven expertise who can report illegal activities for fast analysis ('trusted flaggers')	X			
7. Detect illegal content, goods or services				
8. In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law	X			
9. Request professional users to identify themselves clearly ('know your customer' policy)	X			

	<b>YES, BY ALL ONLINE PLATFORMS, ACCORDING TO THE ACTIVITIES THEY HOSTING, SELLING GOODS OR SERVICES)</b>	<b>YES, ONLY BY LARGER ONLINE PLATFORMS</b>	<b>YES, ONLY PLATFORMS AT PARTICULAR RISK OF EXPOSURE TO ILLEGAL ACTIVITIES BY THEIR USERS</b>	<b>SUCH MEASURES SHOULD NOT BE LEGALLY REQUIRED</b>
10. Provide technical means allowing professional users to comply with their obligations (e.g. enable them to publish on the platform the pre-contractual information consumers need to receive in accordance with applicable consumer law)	X			
11. Inform consumers when they become aware of product recalls or sales of illegal goods	X			
12. Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities				X
13. Be transparent about their content policies, measures and their effects	X			
14. Maintain an effective 'counter-notice' system for users whose goods or content is removed to dispute erroneous decisions	X			
15. Other. Please specify				

**Q14.** Please elaborate, if you wish to further explain your choices.

Response from Open Society European Policy Institute

The digital economy has achieved a considerable degree of complexity, particularly in terms of the legal and economic roles of different actors. Any EU law regulating the digital economy must therefore take into consideration the heterogeneity of actors and be carefully calibrated to achieve all of the public policy goals it sets out to accomplish.

A reasonable approach to designing a modern legislative framework could distinguish between different types of economic intermediation. The distinction is necessarily based on the object of the intermediation, whether it is a good, a service, or user-generated content (text, audio, images). It is important to calibrate carefully the obligations imposed upon platforms that intermediate the exchange of user-generated content, as any regulatory measure could have a potentially detrimental effect on freedom of expression.

A further distinction seems necessary based on the roles and activities of the intermediaries, and the power and control they exercise over the two-sided markets they typically create. Not all platforms influence and control the parties that trade in goods and services or exchange information through their networks. Some have relatively hands-off models, while others very actively promote, curate, amplify and monetise the content that users create, access and share.

In addition to legal obligations that may stem from the Digital Services Act, such distinctions between different types of platforms are crucial to ensure that digital platforms comply with the right applicable set of legal frameworks that are relevant for their economic activity.

Taking into account the different platform models and their varying impact on society, the following general considerations seem reasonable as a general policy approach:

- Online marketplaces that create multi-sided markets for the trading of goods, whether or not the same company is involved as a first-party trader too, should be legally mandated to ensure that the goods sold through it comply with safety legislation. They should also ensure that all parties are aware of and comply with their respective obligations under general consumer law as well as any other applicable laws (eg: financial or banking laws depending on the financial and payment services involved).
- Platforms which intermediate the provision of professional services should be legally mandated to ensure that the provision of services they intermediate comply with all relevant consumer, employment and financial laws.
- Platforms that intermediate the exchange of user-generated content should put in place an effective and transparent notice and action mechanism, with its corresponding counter-notice, as the basic first element for reporting illegal content. For this type of platforms, further thoughts about their obligations are spelled out in other questions of this questionnaire.
- Law enforcement requests should follow due process through the appropriate legal framework involving courts or other independent judicial authorities, not the platforms' notice and action mechanism. Allowing law enforcement authorities to use the same system as users would bypass the necessary safeguards that are intended to create checks and balances on the powers of the State.

Some online platforms combine the provision of two or more of the activities described above. The EU's legal framework should be detailed and nimble enough to be able to take into account those type of actors that offer multiple different services online in a combined manner.

**Q15.** 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

**Q16.** 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?

Response from Open Society European Policy Institute

The use of automated tools for detection of user-generated content must never be a legal obligation, as the ample case law from the ECJ has made abundantly clear. As EDRI rightly argues, such automatic 'filters are not equipped to make complex judgments on the legality of content posted online. They do not understand the context in which content is published and shared, and as a result, they can often make mistakes. Such algorithmic tools do not take proper account of the legal use of the content, for example for educational, artistic, journalistic or research purposes, for expressing polemic, controversial and dissident views in the context of public debates or in the framework of awareness raising activities. They risk accidentally suppressing legal speech, with exacerbated impacts on already marginalised individual internet users.'<sup>1</sup>

For platforms offering goods or services, the risk to freedom of expression is much less, and therefore the threshold of protection is different. There, automated means of detecting the reappearance of goods or services that have been illegal may be an efficient way of detecting fraud and security risks. Users should always have a way to seek redress if they think the deletion is incorrect.

---

1 EDRI, <https://edri.org/trilogues-on-terrorist-content-upload-or-re-upload-filters-eachy-peachy/>

**Q17.** 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:

- Digital services established outside of the Union?
- Sellers established outside of the Union, who reach EU consumers through online platforms?

Response from Open Society European Policy Institute

The Digital Services Act should capture in its scope any service being offered to individuals inside the Union, regardless of where the service provider is based. Similarly, sellers targeting their products at consumers inside the Union through online platforms should also be bound by Digital Services Act rules, just as they are by rules in the consumer acquis.

On the other hand, content takedown orders should be limited in geographical scope. Global take down orders should be prevented to avoid a race to the bottom between countries, as argued nicely by EFF<sup>2</sup>.

**Q18.** 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.?

Response from Open Society European Policy Institute

When companies provide digital services whereby they only perform a mere transit function (DNS, cloud, P2P), they should bear no responsibility for the content transported.

When companies provide mere hosting services (CDNs, cloud storage, etc.), they should only be held liable if they fail to respond to court orders declaring the illegality of the content they host.

**Q19.** 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?

Response from Open Society European Policy Institute

The Digital Services Act will require a dedicated, efficient, and strong enforcement architecture. The authorities in charge of such enforcement must be properly resourced and trained to be able to oversee the activities of online platforms and enforce their obligations under the DSA. Often, overseeing the obligations in the DSA will involve other sectorial regulatory authorities and/or the judiciary. EU and National institutions must ensure that that all authorities and bodies involved are properly scoped, resourced and ready to protect and enforce individuals' rights. For more details, please refer to the last section of this questionnaire.

---

2 <https://www.eff.org/deeplinks/2020/07/effs-eu-policy-principles-platform-liability-and-monitoring>

**Q20.** 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?

Response from Open Society European Policy Institute

Platforms can moderate online content beyond what has been declared illegal. Content moderation systems must be transparent and built based on international human rights principles, particularly legality, necessity, proportionality and legitimacy. Any removals must be transparent and contestable. Platforms should also have a mechanism for users to contest the removal and restore the content.

For more detailed recommendations on how platforms should build their content moderation systems, please refer to groups such as Access Now<sup>3</sup>, Article 19<sup>4</sup>, and EFF<sup>5</sup>.

**Q21.** 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.

Response from Open Society European Policy Institute

Examples of good content moderation practices for legal but potentially harmful content are scarce. Unfortunately, most large internet platforms largely fail<sup>6</sup> to develop efficient, human rights-centred content moderation practices. The use of automated means to moderate content aggravates existing problems and creates new ones. And it is hardly contestable by users<sup>7</sup> that may be affected by it.

To help improve the situation, beyond any regulatory efforts that will come from the EU, online platforms should follow at a minimum the recommendations from groups like Article 19<sup>8</sup> and Access Now<sup>9</sup>.

- Design terms of service and content moderation policies based on human rights by design, including international freedom of expression standards and due process. Do not wait for abuses to occur. Ensure content moderation decisions are predictable and understandable.
- Consult experts and civil society organisations, particularly those representing the voices of the most disenfranchised, racialised or vulnerable groups throughout the process of creation, evaluation, and update of Terms of Service and community guidelines.
- Evaluate the impact of their content moderation policies and practices. Cooperate with external researchers and experts to do so.

---

3 <https://www.accessnow.org/cms/assets/uploads/2020/03/Recommendations-On-Content-Governance-digital.pdf>

4 [https://www.article19.org/wp-content/uploads/2018/03/Self-regulation-and-%E2%80%98hate-speech%E2%80%99-on-social-media-platforms\\_March2018.pdf](https://www.article19.org/wp-content/uploads/2018/03/Self-regulation-and-%E2%80%98hate-speech%E2%80%99-on-social-media-platforms_March2018.pdf)

5 <https://www.eff.org/deeplinks/2019/04/content-moderation-broken-let-us-count-ways>

6 <https://www.eff.org/deeplinks/2019/04/content-moderation-broken-let-us-count-ways>

7 <https://www.eff.org/deeplinks/2020/04/automated-moderation-must-be-temporary-transparent-and-easily-appealable>

8 [https://www.article19.org/wp-content/uploads/2018/03/Self-regulation-and-%E2%80%98hate-speech%E2%80%99-on-social-media-platforms\\_March2018.pdf](https://www.article19.org/wp-content/uploads/2018/03/Self-regulation-and-%E2%80%98hate-speech%E2%80%99-on-social-media-platforms_March2018.pdf)

9 <https://www.accessnow.org/cms/assets/uploads/2020/03/Recommendations-On-Content-Governance-digital.pdf>

**Q22.** Please rate the necessity of the following measures for addressing the spread of disinformation online. Please rate from 1 (not at all necessary) to 5 (very necessary) each option below.

	1 (NOT AT ALL NECESSARY)	2	3 (NEUTRAL)	4	5 (VERY NECESSARY)	I DON'T KNOW / NO ANSWER
1. Transparently inform consumers about political advertising and sponsored content, in particular during electoral periods					X	
2. Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with users' complaints					X	
3. Tackle the use of fake-accounts, fake engagements, bots and inauthentic users' behaviour aimed at amplifying false or misleading narratives					X	
4. 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					X	
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					X	

	1 (NOT AT ALL NECESSARY)	2	3 (NEUTRAL)	4	5 (VERY NECESSARY)	I DON'T KNOW / NO ANSWER
6. Adapted risk assessments and mitigation strategies undertaken by online platforms				X		
7. Ensure effective access and visibility of a variety of authentic and professional journalistic sources					X	
8. Auditing systems over platforms' actions and risk assessments					X	
9. 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.					X	
10. Other, please specify					X	

Response from Open Society European Policy Institute

EU and national policy-makers should engage on the following priority measures:

- Regulate the transparency of online advertising, including by requiring mandatory and comprehensive ad archives. Mandate the labelling of bots and of content disseminated by State-controlled entities, institutions and political parties.
- Ensure the enforcement of the GDPR towards online platforms and political parties, including restrictions on micro-targeting (such as on the basis of sexual orientation, religion, disability, ethnicity) and fines for noncompliance.
- Use the DSA to disincentives the widespread dissemination of disinformation and divisive content to push the market towards more human rights-respecting, democracy-enabling business models.



- Create an access to data framework that respects individuals' data protection rights to enable civil society, researchers and journalists to analyse and evaluate content being shared on platforms for public interest auditing and oversight. For more info, see points by European Policy Centre (EPC) & AlgorithmWatch<sup>10</sup>.
- Algorithmic systems must be auditable and overseen. EU Regulation should enable third-party algorithm inspection in the public interest.
- Establish a decentralised cooperation framework on disinformation that includes necessary funding schemes in support of civil society organisations working to combat disinformation across Europe. See more from EU DisinfoLab<sup>11</sup>.
- The Commission should take proactive steps against the 'disinformation industry' (companies dedicated to the sale of fake profiles, 'click farms', 'like farms', etc.).
- Empower an independent auditing body specifically tasked with overseeing and monitoring online platforms are doing to address disinformation on their networks.
- The Commission should seek to establish best practices in upgrading electoral law for the digital age.
- Complete the ePrivacy Regulation reform to ensure that all individuals enjoy the right not to be tracked online.
- Create a binding Code of Conduct for all European-wide political parties to self-enforce a system of internal sanctioning for any disinformation generated and disseminated through their own ranks.
- Member States should guarantee individuals' right to access to information and publish all necessary information about any matter of public interest.
- The Commission should urgently scrutinise any emergency power adopted by Member States that gives national institutions the power to disproportionately criminalise the production and dissemination of disinformation. For further information, see this report from AccessNow<sup>12</sup>.

---

10 [https://algorithmwatch.org/wp-content/uploads/2020/06/GoverningPlatforms\\_IViR\\_study\\_June2020-AlgorithmWatch-2020-06-24.pdf](https://algorithmwatch.org/wp-content/uploads/2020/06/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf)

11 <https://www.disinfo.eu/advocacy/our-position-on-the-joint-communication-tackling-covid-19-disinformationgetting-the-facts-right>

12 <https://www.accessnow.org/cms/assets/uploads/2020/04/Fighting-misinformation-and-defending-freeexpression-during-COVID-19-recommendations-for-states-1.pdf>

**Q23.** What would be effective measures service providers should take, in your view, for protecting the freedom of expression of their users? Please rate from 1 (not at all necessary) to 5 (very necessary).

	1 (NOT AT ALL NECESSARY)	2	3 (NEUTRAL)	4	5 (VERY NECESSARY)	I DON'T KNOW / NO ANSWER
1. High standards of transparency on their terms of service and removal decisions					X	
2. Diligence in assessing the content notified to them for removal or blocking					X	
3. Maintaining an effective complaint and redress mechanism					X	
4. Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended					X	
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					X	
6. Enabling third party insight – e.g. by academics – of main content moderation systems					X	
7. Other. Please specify						

**Q24.** In your view, is there a need for enhanced data sharing between online platforms and authorities, within the boundaries set by the General Data Protection Regulation? Please select the appropriate situations, in your view:

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

**Q25.** Please explain. What would be the benefits? What would be concerns for the companies, consumers or other third parties?

Response from Open Society European Policy Institute

See above regarding integration with third-party mechanisms.

**Q26.** 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)?

Response from Open Society European Policy Institute

Any financial sanctions would have to follow an approach similar to that of the GDPR, where the company is fined over its global turnover, and the amount has to be significant to be a real deterrent and incentivise to comply.

That said, it is likely that however high the fines may be, they could hardly represent a significant threat to the profits made by the biggest online platforms through their current business model. Fines should be therefore accompanied with technical and structural remedies such as mandatory data portability, interconnections and/or interoperability. It is the perspective of users leaving their platforms in droves that could become a strong incentive for those platforms to move towards a more rights-respecting business models in the medium to long term.

For rideshare firms, the transport license to operate should be dependent upon compliance with the relevant applicable legal frameworks, in particular regarding employment and those stemming from the upcoming DSA.

**Q27.** Are there other points you would like to raise?

Response from Open Society European Policy Institute

Regarding the promotion of media and trustworthy on online intermediary services (such as search engines, social media, and aggregators), this would be in principle a positive development. However, in reality this would require widespread agreement on standards for qualifying 'independence' and 'trustworthiness' in a highly charged and politically divisive environment. We therefore err towards a Newsguard-style browser plugin model, which automatically flags search results and social media posts with green, red or yellow flags, and reveals further factual details such as their ownership and funding source when hovering over them.

Its broad inclusiveness is a strength: although it flags as green sources that many would consider dubious (i.e. Daily Mail in the UK), the plugin provides extensive background on the entities behind news and posts, and is very effective at red-flagging egregious and manipulative sources that readers may be unfamiliar with, e.g. sources from other countries.

The real power of this plugin model comes from the prospect of including it in browsers, rolling it out in an update, and switching it on by default (leaving the possibility for users to opt-out).

Boosting news sources flagged as 'green' through fair and equitable upranking on browser search results and social media platforms could also be an effective way to promote independent and reliable journalism.

## II. REVIEWING THE LIABILITY REGIME OF DIGITAL SERVICES ACTING AS INTERMEDIARIES?

The liability of online intermediaries is a particularly important area of internet law in Europe and worldwide. The E-Commerce Directive harmonises the liability exemptions applicable to online intermediaries in the single market, with specific provisions for different services according to their role: from Internet access providers and messaging services to hosting service providers.

The previous section of the consultation explored obligations and responsibilities which online platforms and other services can be expected to take – i.e. processes they should put in place to address illegal activities which might be conducted by users abusing their service. In this section, the focus is on the legal architecture for the liability regime for service providers when it comes to illegal activities conducted by their users. The Commission seeks informed views on how the current liability exemption regime is working and the areas where an update might be necessary.

**Q28.** 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.

Response from Open Society European Policy Institute

The intermediary liability regime is the cornerstone of internet regulation designed to foster free speech online. It is therefore important for the EU to maintain such a regime, adapting it to a new reality that requires updated definitions, concepts, and sets of obligations.

As argued further above, if an online platform’s service does not involve hosting content but only providing an access or transit service (mere conduit, access provider, search engine, etc), the platform should never be held liable for the content in transfers. In addition, there should not be any general monitoring obligations or obligations to use any type of proactive measure to the content they transfer.

If an online platform’s service involves hosting of content, the platform’s liability regarding the user-generated content it hosts must be limited to where the platform does not comply with a court order mandating the take down of a specific piece of content.

For hosting services, the liability exemption for third parties’ content or activities is conditioned by a knowledge standard (i.e. when they get ‘actual knowledge’ of the illegal activities, they must ‘act expeditiously’ to remove it, otherwise they could be found liable).

**Q29.** 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.

Response from Open Society European Policy Institute

The distinction between 'active' and 'passive' intermediaries is outdated. The new legal framework should drop the distinction between active and passive and focus on the type of services offered by each type of platforms, and associate legal rights and obligations to those.

**Q30.** 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.

Response from Open Society European Policy Institute

Yes, the prohibition of any general monitoring is key.

New legislative initiatives should never impose general monitoring obligations on digital platforms or incentivise them to use automated filtering systems that endanger the freedom to receive and impart information as well as data protection rights and are incompatible with EU law. Outsourcing legality decisions on speech governance, for instance, to corporate actors, without judicial oversight or proper redress mechanism, would translate into a dangerous privatisation of law enforcement activities.

## III. WHAT ISSUES DERIVE FROM THE GATEKEEPER POWER OF DIGITAL PLATFORMS?

There is wide consensus concerning the benefits for consumers and innovation, and a wide range of efficiencies, brought about by online platforms in the European Union's Single Market. Online platforms facilitate cross-border trading within and outside the EU and open entirely new business opportunities to a variety of European businesses and traders by facilitating their expansion and access to new markets. At the same time, regulators and experts around the world consider that large online platforms are able to control increasingly important online platform ecosystems in the digital economy. Such large online platforms connect many businesses and consumers. In turn, this enables them to leverage their advantages – economies of scale, network effects and important data assets- in one area of their activity to improve or develop new services in adjacent areas. The concentration of economic power in the platform economy creates a small number of 'winner-takes it all/most' online platforms. The winner online platforms can also readily take over (potential) competitors and it is very difficult for an existing competitor or potential new entrant to overcome the winner's competitive edge.

The Commission announced that it 'will further explore, in the context of the Digital Services Act package, ex ante rules to ensure that markets characterised by large platforms with significant network effects acting as gatekeepers, remain fair and contestable for innovators, businesses, and new market entrants'.

This module of the consultation seeks informed views from all stakeholders on this framing, on the scope, the specific perceived problems, and the implications, definition and parameters for addressing possible issues deriving from the economic power of large, gatekeeper platforms.

The Communication 'Shaping Europe's Digital Future' also flagged that 'competition policy alone cannot address all the systemic problems that may arise in the platform economy'. Stakeholders are invited to provide their views on potential new competition instruments through a separate, dedicated open public consultation that will be launched soon.

In parallel, the Commission is also engaged in a process of reviewing EU competition rules and ensuring they are fit for the modern economy and the digital age. As part of that process, the Commission has launched a consultation on the proposal for a New Competition Tool aimed at addressing the gaps identified in enforcing competition rules. The initiative intends to address as specific objectives the structural competition problems that prevent markets from functioning properly and that can tilt the level playing field in favour of only a few market players. This could cover certain digital or digitally enabled markets, as identified in the report by the Special Advisers and other recent reports on the role of competition policy, and/or other sectors. As such, the work on a proposed new competition tool and the initiative at stake complement each other. The work on the two impact assessments will be conducted in parallel in order to ensure a coherent outcome. In this context, the Commission will take into consideration the feedback received from both consultations. We would therefore invite you, in preparing your responses to the questions below, to also consider your response to the parallel consultation on a new competition tool.

**Q31.** To what extent do you agree with the following statements?

	FULLY AGREE	SOMEWHAT AGREE	NEITHER AGREE NOT DISAGREE	SOMEWHAT DISAGREE	FULLY DISAGREE	I DON'T KNOW / NO REPLY
1. Consumers have sufficient choices and alternatives to the offerings of online platforms.					X	
2. It is easy for consumers to switch between services provided by online platform companies and use same or similar services provider by other online platform companies ("multi-home").					X	
3. It is easy for individuals to port their data in a useful form for alternative service providers outside of an online platform.					X	
4. There is sufficient level of interoperability between services of different online platform companies.					X	
5. There is an asymmetry of information between the knowledge of online platforms about consumers, which enables them to target them with commercial offers, and the knowledge of consumers about market conditions.	X					
6. It is easy for innovative SME online platforms to expand or enter the market.				X		



	FULLY AGREE	SOMEWHAT AGREE	NEITHER AGREE NOT DISAGREE	SOMEWHAT DISAGREE	FULLY DISAGREE	I DON'T KNOW / NO REPLY
7. Traditional businesses are increasingly dependent on a limited number of very large online platforms.	X					
8. There are imbalances in the bargaining power between these online platforms and their business users.	X					
9. Businesses and consumers interacting with these online platforms are often asked to accept unfavourable conditions and clauses in the terms of use/contract with the online platforms.	X					
10. Certain large online platform companies create barriers to entry and expansion in the Single Market (gatekeepers).	X					
11. Large online platforms often leverage their assets from their primary activities (customer base, data, technological solutions, skills, financial capital) to expand into other activities.	X					
12. When large online platform companies expand into such new activities, this often poses a risk of reducing innovation and deterring competition from smaller innovative market operators.	X					

## MAIN FEATURES OF GATEKEEPER ONLINE PLATFORM COMPANIES AND MAIN RELEVANT CRITERIA FOR ASSESSING THEIR ECONOMIC POWER

**Q32.** Which characteristics are relevant in determining the gatekeeper role of large online platform companies? Please rate each criterion identified below from 1 (not relevant) to 5 (very relevant):

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

**Q33.** Please explain your answer. How could different criteria be combined to accurately identify large online platform companies with gatekeeper role?

Response from Open Society European Policy Institute

The internet economy has developed in a way in which many parts of it have rallied around tight ecosystems of services, where few companies control the different markets, user groups, and content shared within those ecosystems. All too often, only one or two companies have a tight grip over the ecosystem around them. This phenomenon has happened across different layers of the internet, from end user-oriented services such as social media platforms, double-sided platforms, advertising networks, and all sorts of cloud-based service providers. In markets such as mobile operating systems, online search and social media, the share controlled by one or two companies is over 90% of the market (Furman et al., Unlocking Digital Competition – 2019).

With the current trend, the ideal of a decentralised, highly innovative and dynamic, user-centric, freedoms and rights-enabling internet becomes more distant as power is increasingly accumulated in the hands of a wealthy few so-called digital gatekeepers.

The criteria listed in the table above is a good start of what a regulator should look at to detect gatekeeping. Translating them into a formula that regulators can use to detect gatekeeping will not be an easy task and requires careful consideration. The EU co-legislator could look into similar models

that aim to identify situations of unchecked dominance, such as the Significant Market Power regime in telecoms law.

To begin with, regulators should look at the different assets of any given player (user base, data, assets in adjacent markets), their ability to raise entry barriers and to leverage assets onto other markets or sub-markets, constitute a position that has an important effect on competitors, innovators, users, rights and democracy.

Useful proposals on how to design such a new asymmetric regime for intervention have been made by regulatory bodies such as BEREC<sup>13</sup> and ARCEP<sup>14</sup>.

**Q34.** 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:

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

**Q35.** Are there specific issues and unfair practices you perceive on large online platform companies?

Response from Open Society European Policy Institute

There are many practices that digital platforms have been deploying for many years and which unfortunately remain unaddressed. Many of these practices are exacerbating existing gatekeeping problems and worsening the stronghold of a few actors over the ecosystems they control.

13 [https://bereg.europa.eu/eng/document\\_register/subject\\_matter/bereg/others/9411-berec-response-to-the-public-consultation-on-the-digital-services-act-package-and-the-new-competition-tool](https://bereg.europa.eu/eng/document_register/subject_matter/bereg/others/9411-berec-response-to-the-public-consultation-on-the-digital-services-act-package-and-the-new-competition-tool)

14 [https://www.arcep.fr/uploads/tx\\_gspublication/consultation-DSA-reponse-ARCEP\\_sept2020.pdf](https://www.arcep.fr/uploads/tx_gspublication/consultation-DSA-reponse-ARCEP_sept2020.pdf)

Some of those problematic practices are:

- Lack of any meaningful interoperability, closing up the service or platform from being connected with other relevant services.
- Self-preferencing, where a platform that is supposed to provide search results of web links, content, products or services, artificially gives preference to its own products or services in downstream or related markets.
- Wide-spread privacy and data protection violations as the basis of the platform's business activity. Unfortunately, surveillance capitalism has become the norm in the internet economy, which creates both competition and data protection problems.
- Forced consent to combine personal data from different services from the same company, not only violating users' fundamental rights, but also worsening the 'ecosystemisation effect'.
- Vertical integration between different services of the same group, which can be problematic in and of itself. Often this may happen in combination of with self-preferencing too.
- Abusive terms on operating systems and App Stores that suffocate app developers and competitors, hampering innovation and reducing consumer choice.
- Tying of downstream products and services, as has happened in the past with desktop operating systems and is now common on mobile operating systems (eg: Android + G-Suite).
- #DarkPatterns – or the conscious use of design and engineering of services and websites to trick users into sharing more data than they want or purchasing services they don't really want.

For a more detailed list of problematic practices, please refer to ARCEP's helpful list<sup>15</sup>.

**Q36.** In your view, what practices related to the use and sharing of data in the platforms' environment are raising particular challenges?

Response from Open Society European Policy Institute

- As mentioned above, the widespread, illegal and unaccountable online tracking of users must be addressed. Online tracking has become a pervasive, widespread practice across the internet, and it is imperative that an efficient regulatory solution is found to counteract this phenomenon. Users should be able to oppose online tracking, which should only happen with their explicit, informed and unambiguous consent. If necessary, the EU should review the possibility of a Do Not Track standard.
- Alternative business models are possible and should be incentivised. As recently as January 2020, Dutch public broadcaster NPO decided to switch off 3<sup>rd</sup> party tracking and focus exclusively on contextual advertising, and not only have its revenues not decreased because of that change, they have in fact increased. These kind of initiatives demonstrate the viability of alternative advertising models that generate sufficient revenue for the parties involved, and which do not come with the

---

15 [https://www.arcep.fr/uploads/tx\\_gspublication/consultation-DSA-reponse-ARCEP\\_sept2020.pdf](https://www.arcep.fr/uploads/tx_gspublication/consultation-DSA-reponse-ARCEP_sept2020.pdf) (page 7)

widespread pernicious effects that the tracking-based, behavioural model has brought to the internet.<sup>16</sup>

- Micro-targeting has proved to be a very perilous practice as it severely affects the digital public sphere and public debate. Micro-targeting needs to be disincentivised and restricted through regulation by clearly delimiting through regulation the conditions under which it can be used. An open society cannot be based on a system where in order get political messages out to the public there is a need for a widespread violation of people's fundamental rights.
- Restricting and disincentivising micro-targeting would be a clear societal signal to dominant platforms that their business model should evolve and move away from one solely based on targeted, behavioural advertising, as it has naturally led to a situation where the most extreme, controversial and divisive content gets disproportionately amplified.
- The Ad Tech market has become too complex to oversee and police. There is too much unchecked sharing of personal data, with too many parties involved, and without any empowerment of the individual whose personal data is being traded. Real time bidding is likely illegal under current legislation and should become a priority for Data Protection Authorities and any other relevant regulators.
- Large online platforms increasingly mix the data they obtain from different services, making it more difficult for regulators to oversee their activities, and for a competition authority to order a functional or structural separation<sup>17</sup>.

**Q37.** 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?

Response from Open Society European Policy Institute

- Large platforms set the standards in the market with regards to users' rights to privacy, data protection and freedom of expression. This is possible because of the lack of alternatives and because of the immense imbalance of power between them and their users.
- Opaque data harvesting, content curation and distribution, and micro-targeting have contributed to create an unhealthy digital public sphere, without transparency nor open debate, and a public discourse that is directly in the hands of platforms' algorithms. In a way, they have become the operating systems and app stores of democracy, directly affecting media pluralism and democratic participation.
- Gatekeepers with a tight control over the ecosystem they operate (e.g. Apple, Google) negatively affect consumers by constraining innovation and reducing consumer choice in those markets where they compete vertically.

<sup>16</sup> <https://brave.com/npo/>

<sup>17</sup> J Tirole, Competition and the Industrial Challenge for the Digital Age, Institute for Fiscal Studies 'Inequalities in the Twenty-First Century' review background paper, 3 April 2020 - [https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/by/tirole/competition\\_and\\_the\\_industrial\\_challenge\\_april\\_3\\_2020.pdf](https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/by/tirole/competition_and_the_industrial_challenge_april_3_2020.pdf)

- Gatekeepers with unchecked power over the marketplaces they create (e.g. Amazon) negatively affect consumers by making it difficult for third party sellers to compete with their direct sales. They also decrease consumer safety by having weak compliance policies with safety regulations.
- Different economic harms occur due to the lack of competition. As reported by the UK's Competition and Markets Authority (Online platforms and digital advertising, Competition and Markets Authority, 2020), as direct harms, consumers face reduced innovation, restricted choice, lower quality and limited control over data. As indirect harms: via advertisers, consumers pay higher prices for goods and services across the economy; via publishers, the quality and range of important content such as news articles could decline, to detriment of democracy; via other markets, consumers could miss out on new products and services in emerging markets.

## REGULATION OF LARGE ONLINE PLATFORM COMPANIES ACTING AS GATEKEEPERS

**Q38.** 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

Response from Open Society European Policy Institute

*Ex post* competition rules have demonstrated to be insufficient, and enforcement of these rules, too slow. Time and again, by the time competition regulators impose remedies and sanctions and courts validate them if challenged, the harm done to markets and to society is already irreversible.

*Ex post* competition rules are only capable of addressing those cases that authorities consider a priority, but similar problematic conducts exist in other players and authorities cannot cope with the size of the challenge.

By establishing certain asymmetric rules applicable only to those online platforms that meet a set of criteria that identify them as problematic gatekeepers for markets and society, the EU will be actively contributing to restore competition and innovation in the digital economy, defend fundamental rights and promote plurality and open democratic debate.

To promote an open, decentralised, thriving digital ecosystem that creates value for society as a whole, one that empowers individuals, traditional economic and regulatory policy will not suffice. The state of the digital economy requires obligations more and better interoperability between services, more and better security policies, and strong enforcement of privacy and data protection rights. Dedicated regulatory rules have therefore become essential.

**Q39.** 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

**Q40.** Please explain your reply and, if possible, detail the types of prohibitions that should in your view be part of the regulatory toolbox.

Response from Open Society European Policy Institute

The European Commission should look into possible forms of partial or total bans of the problematic practices identified (in question 81) above.

For instance, the European Commission should explore the possibility of prohibiting the use of targeted advertising altogether, or at least of the most pernicious forms of real time bidding. Alternatively, a ban on the use of targeted advertising only on Google and Facebook could be explored. For more information, see American Economic Liberties Project report<sup>18</sup>.

**Q41.** Do you believe that such dedicated rules should include obligations on large online platform companies with gatekeeper role?

- Yes
- No
- I don't know

**Q42.** Please explain your reply and, if possible, detail the types of obligations that should in your view be part of the regulatory toolbox.

Response from Open Society European Policy Institute

Different types of problematic practices in the market and different platforms will require different obligations.

#### **Interoperability**

The European Commission should look into interoperability as a matter of priority and carefully analyse the opportunities that different forms of interoperability requirements would offer. The EU co-legislator should look into different forms of interoperability across different concentrated digital markets and use the DSA to impose certain forms of interoperability onto large digital gatekeepers. Businesses and civil society alike recognise the value of interoperability as a regulatory tool that will

---

<sup>18</sup> <https://www.economicliberties.us/our-work/addressing-facebook-and-googles-harms-through-a-regulated-competition-approach/>

bring more choice and innovation to these highly concentrated markets. For more information, see joint letter from civil society organisations and online businesses<sup>19</sup>.

Different forms of interoperability would allow breaking into companies' dominance in a way in which all market actors win. It also enables combinations of component products and services that best meet user needs, increasing innovation and/or reducing prices. Many argue that interoperability based on standards reduce the incentive to operate. Under the current conditions, as described by the UK's Competition and Markets Authority (Online platforms and digital advertising, Competition and Markets Authority, 2020), the use of open standards for the most common functions of for example social media platforms would enable competitors to reach a wider audience, thus in fact increasing the incentive of all market players to innovate. It is important to remember that multi-homing is not a valid alternative to interoperability, as multi-homing is not cost-free for users. For a thorough analysis of the benefits of different forms of interoperability, please refer to Professor Ian Brown's report 'Interoperability as a tool for competition regulation'<sup>20</sup>.

Interoperability through Application Programming Interfaces (APIs) will also be essential to implement many solutions regarding online content, so that trusted flaggers, fact-checkers and researchers can access the necessary data. For these purposes, though, the obligations should not be limited to digital gatekeepers only.

The European Commission could also consider different forms of **structural and/or functional separation** (see American Economic Liberties Project April 2020 for a list of possible interventions in this realm and the potential benefits of each one), as tools for case-by-case remedies (as identified below).

As highlighted earlier, the EU should consider the implementation of a **Do Not Track mechanism** in Europe.

**Q43.** 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

**Q44.** If yes, please explain your reply and, if possible, detail the types of case by case remedies.

Response from Open Society European Policy Institute

In order to be as adaptive and nimble as possible, this new layer of competition rules should include both asymmetric horizontal rules as well as dedicated case-by-case remedies.

19 <https://www.eff.org/document/letter-vestager-interoperability>

20 <https://osf.io/preprints/lawarxiv/fbvxd/>



Certain companies, and in particular Facebook, will likely need dedicated remedies. As explained by the CMA (Online platforms and digital advertising, Competition and Markets Authority, 2020), the characteristics of Facebook's activities and market position and the way users behave, have turned it into a must-have platform, and developing alternatives has become increasingly difficult.

Case-by-case remedies could include: non-discrimination and/or the prohibition of self-preferencing, access to assets such as data sets, interoperability through APIs or open standards, as explained above, and different forms of functional or structural separation.

**Q45.** 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

**Q46.** 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.

Response from Open Society European Policy Institute

Yes, it is essential that the Digital Services Act be designed to look at and address a myriad of societal issues caused by a small group of digital gatekeepers, and not just their impact on the market from an exclusively economic perspective.

As rightly argued in a joint statement of civil society organisations, 'this small number of large online platforms not only act as economic gatekeepers, but also as "fundamental rights" gatekeepers. Through their business models, their terms of services and community guidelines, these platforms set standards in the market with regards to, among others, consumers' rights to privacy, data protection and freedom of expression. The impact of these platforms' behaviours and business models on the guarantee of fundamental rights in the digital single market is a major challenge for the EU, and the European Commission should include it in its understanding of the problem it aims to fix with these welcomed initiatives.'<sup>21</sup>

---

21 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers/F535488>

**Q47.** 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?

Response from Open Society European Policy Institute

A data access regime is necessary to enable competition and better consumer control over their personal data. For some helpful suggestions, see BEUC's report on the matter<sup>22</sup>.

In addition, an access to data framework that respects individuals' data protection rights is necessary to enable researchers and journalists to analyse and evaluate content being shared on platforms. For more recommendations, see the report by EPC & AlgorithmWatch<sup>23</sup>.

**Q48.** 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

**Q49.** 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

---

22 [https://www.beuc.eu/publications/beuc-x-2019-068\\_european\\_data\\_policy.pdf](https://www.beuc.eu/publications/beuc-x-2019-068_european_data_policy.pdf)

23 [2] [https://algorithmwatch.org/wp-content/uploads/2020/06/GoverningPlatforms\\_IViR\\_study\\_June2020-AlgorithmWatch-2020-06-24.pdf](https://algorithmwatch.org/wp-content/uploads/2020/06/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf)

**Q50.** Taking into consideration the parallel consultation on a proposal for a New Competition Tool focusing on addressing structural competition problems that prevent markets from functioning properly and tilt the level playing field in favour of only a few market players. Please rate the suitability of each option below to address market issues arising in online platforms ecosystems. Please rate the policy options below from 1 (not effective) to 5 (most effective).

	1 (NOT EFFECTIVE)	2 (SOMEWHAT EFFECTIVE)	3 (SUFFICIENTLY EFFECTIVE)	4 (VERY EFFECTIVE)	5 (MOST EFFECTIVE)	NOT APPLICABLE / NO RELEVANT EXPERIENCE OR KNOWLEDGE
1. Current competition rules are enough to address issues raised in digital markets	X					
2. There is a need for an additional regulatory framework imposing obligations and prohibitions that are generally applicable to all large online platforms with gatekeeper power					X	
3. There is a need for an additional regulatory framework allowing for the possibility to impose tailored remedies on individual large online platforms with gatekeeper power, on a case- by-case basis					X	
4. There is a need for a New Competition Tool allowing to address structural risks and lack of competition in (digital) markets on a case-by- case basis.					X	
5. There is a need for combination of two or more of the options 2 to 4.					X	

**Q51.** 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.

Response from Open Society European Policy Institute

Both an asymmetric (only to large platforms) horizontal (to *any* large platform) as well as a regime of tailored remedies on case-by-case basis (e.g. for Facebook, Google and Amazon) will be necessary as part of the DSA.

This new regulatory framework should be complementary to the New Competition Tool, which should be horizontal and symmetric, and allow European Competition Authorities to intervene in markets before they tip.

## IV. OTHER EMERGING ISSUES AND OPPORTUNITIES, INCLUDING ONLINE ADVERTISING AND SMART CONTRACTS

Online advertising has substantially evolved over the recent years and represents a major revenue source for many digital services, as well as other businesses present online, and opens unprecedented opportunities for content creators, publishers, etc. To a large extent, maximising revenue streams and optimising online advertising are major business incentives for the business users of the online platforms and for shaping the data policy of the platforms. At the same time, revenues from online advertising as well as increased visibility and audience reach are also a major incentive for potentially harmful intentions, e.g. in online disinformation campaigns.

Another emerging issue is linked to the conclusion of 'smart contracts' which represent an important innovation for digital and other services but face some legal uncertainties.

This section of the open public consultation seeks to collect data, information on current practices, and informed views on potential issues emerging in the area of online advertising and smart contracts.

Respondents are invited to reflect on other areas where further measures may be needed to facilitate innovation in the single market. This module does not address privacy and data protection concerns; all aspects related to data sharing and data collection are to be afforded the highest standard of personal data protection.

### ONLINE ADVERTISING

**Q52.** 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

**Q53.** From your perspective, what measures would lead to meaningful transparency in the ad placement process?

Response from Open Society European Policy Institute

Platforms should be asked to establish mandatory ad libraries to provide meaningful information on the origin of the ads, why they are being shown to users, and what demographics they are targeting.

The APIs of advertising libraries should include information about the position of the ads, the content the ads are run next to, the advertiser's identity as well as metrics, engagement and reach, and ad targeting and delivery criteria for all advertising. Some platforms already disclose this kind of information on a voluntary basis; however, regulation should set clear mandatory standards of disclosure for all platforms.

## V. HOW TO ADDRESS CHALLENGES AROUND THE SITUATION OF SELF-EMPLOYED INDIVIDUALS OFFERING SERVICES THROUGH ONLINE PLATFORMS?

Individuals providing services through platforms may have different legal status (workers or self-employed). This section aims at gathering first information and views on the situation of self-employed individuals offering services through platforms (such as ride-hailing, food delivery, domestic work, design work, micro-tasks etc.). Furthermore, it seeks to gather first views on whether any detected problems are specific to the platform economy and what would be the perceived obstacles to the improvement of the situation of individuals providing services through platforms. This consultation is not intended to address the criteria by which persons providing services on such platforms are deemed to have one or the other legal status.

The issues explored here do not refer to the selling of goods (e.g. online marketplaces) or the sharing of assets (e.g. sub-renting houses) through platforms.

### SITUATION OF SELF-EMPLOYED INDIVIDUALS PROVIDING SERVICES THROUGH PLATFORMS

**Q54.** Are there areas in the situation of individuals providing services through platforms which would need further improvements? Please rate the following issues from 1 (no improvements needed) to 5 (substantial issues need to be addressed).

	1 (NO IMPROVEMENTS NEEDED)	2	3	4	5 (SUBSTANTIAL IMPROVEMENTS NEEDED)	I DON'T KNOW / NO ANSWER
1. Earnings					X	
2. Flexibility of choosing when and /or where to provide services		X				
3. Transparency on remuneration					X	
4. Measures to tackle non-payment of remuneration		X				
5. Transparency in online ratings					X	
6. Ensuring that individuals providing services through platforms can contact each other and organise themselves for collective purposes					X	

	1 (NO IMPROVEMENTS NEEDED)	2	3	4	5 (SUBSTANTIAL IMPROVEMENTS NEEDED)	I DON'T KNOW / NO ANSWER
7. Tackling the issue of work carried out by individuals lacking legal permits	X					
8. Prevention of discrimination of individuals providing services through platforms, for instance based on gender, racial or ethnic origin					X	
9. Allocation of liability in case of damage					X	
10. Other, please specify						

**Q55.** Please explain the issues that you encounter or perceive.

Response from Open Society European Policy Institute

We support the points raised by one of our partner organisations, Worker Info Exchange (<https://workerinfoexchange.org/>):

1. Persistent misclassification of workers and/or failure to comply with employment law. The misclassification of workers allows platforms to off-load their market and operational risk to workers, which enables the platform to overstock the market. In turn, this enables the platform to take advantage of economies of scale while workers and communities bear the cost in terms of under-utilisation of their resources, leading to less income, more pollution and traffic congestion due to the increased offer.
2. Minimum wage laws are often weakly enforced if at all. Besides loss of direct pay, holiday pay and parental leave, workers also miss out on private pension and social insurance contributions.
3. Workers suffer due to sudden summary dismissal without right to appeal. There is little incentive for platforms to conduct a proper appeal, and plenty of incentives not to do so. Workers are often dismissed due to declining ratings. For example, Uber drivers who reach a threshold of 4.4 out of 5 are dismissed. Such consumer allocated ratings can be laden with bias and discrimination, and workers have little or no recourse to challenge this.
4. Assaults at work. Drivers and couriers are vulnerable workers often subject to hate, abuse and assault. Union surveys show that 83% of London drivers were subject to hate and 50% have been assaulted. When this happens, operators often take little or no responsibility and too often the police do not take such assaults seriously either. Similarly, such workers often also face criminal damage to their vehicles in such encounters. The workforce, which is mostly made up of ethnic minority or migrant workers, suffer discrimination not only in the committal of the crime, but also in the administration of justice.

5. Safety at work. Misclassification allows platform employers to escape key safety legislation and safety oversight. For example, many such workers classified as self-employed are exempted from the Working Time Directive. They may also escape oversight from national and local occupational health and safety executive authorities. Low pay and high overhead costs for vehicle rental is a dangerous combination leading to long hours and attendant fatigue risk. For example, in the UK union surveys show that it can take an average Uber driver up to 30 hours of work to break even.
6. Platform companies have abused the digital rights of workers by denying key data protection rights including the right to access data, the right to port data to their union's data trust & the right to protection from automated decision making. Worker Info Exchange has recently filed complaints against Uber in the courts in the Netherlands because of failure of Uber to respect access rights under Article 15 of the GDPR as well as the right to explanation for the logic of processing including a clear explanation of the dispatch algorithm. Such firms also flout the rights to protection from automated decision-making under Article 22 of the GDPR, especially relating to dismissals.

**Q56.** Do you think individuals providing services in the 'offline/traditional' economy face similar issues as individuals offering services through platforms?

- Yes  
 No  
 I don't know

**Q57.** Please explain and provide examples.

Response from Open Society European Policy Institute

As our partner Worker Info Exchange finds, many of the problems that exist in the 'offline/traditional' economy have been replicated in models that are offered through online platforms. In some cases, these problems have been exacerbated and worsened.

Individuals with the status of self-employed in the offline economy are often disguised or deliberately misclassified as self-employed in EU Member States, where so-called 'freelance' service providers are often de facto controlled as employees, but not covered by the same level of legal and social protection or remuneration. This has become a standard practice online, as argued above.

Labour conditions in the ridesharing and food delivery sectors have been often poor, which is one of the reasons why platforms have become so successful. If workers had enjoyed good working conditions, they would have been less likely to support emergent platform operators.

Companies offering similar services in the 'offline/traditional' economy have had to adapt and develop services similar to those of online platforms. While this may have some benefits, it also has some detrimental consequences. For instance, while workers had more leverage for collective bargaining power when dealing with traditional firms due to their smaller size and local operations, this power is now increasingly diluted.



**Q58.** In your view, what are the obstacles for improving the situation of individuals providing services

- through platforms?
- in the offline/traditional economy?

Response from Open Society European Policy Institute

We support the points raised by one of our partner organisations, Worker Info Exchange (<https://workerinfoexchange.org/>):

Both in the offline economy and in the platform economy:

1. Weak enforcement of laws protecting workers.
2. Weak regulatory oversight of the sector whether through labour inspectorates, transport regulators or data protection authorities.
3. Poor trade union penetration due to lack of organising effort historically and due to increased dispersal of the workforce engaged via apps.

Specifically, in the platform economy:

1. Immense political lobbying power of platforms and tech giants at EU, national and city level.
2. Hostility to trade unions or any collective negotiations on behalf of workers
3. Distorting effect of massive venture capital investment which has subsidised the disruption and acquisition of markets.
4. Absence of a framework enabling sectoral-level collective bargaining.
5. Data trusts which can better enable and facilitate the collectivisation of the platform workforce.

**Q59.** To what extent could the possibility to negotiate collectively help improve the situation of individuals offering services:

	1 (NO IMPROVEMENTS NEEDED)	2	3	4	5 (SUBSTANTIAL IMPROVEMENTS NEEDED)	I DON'T KNOW / NO ANSWER
1. Earnings					X	
2. Flexibility of choosing when and /or where to provide services		X				
3. Transparency on remuneration					X	
4. Measures to tackle non-payment of remuneration		X				
5. Transparency in online ratings					X	

	1 (NO IMPROVEMENTS NEEDED)	2	3	4	5 (SUBSTANTIAL IMPROVEMENTS NEEDED)	I DON'T KNOW / NO ANSWER
6. Ensuring that individuals providing services through platforms can contact each other and organise themselves for collective purposes					X	
7. Tackling the issue of work carried out by individuals lacking legal permits	X					
8. Prevention of discrimination of individuals providing services through platforms, for instance based on gender, racial or ethnic origin					X	
9. Allocation of liability in case of damage					X	
10. Other, please specify						

**Q60.** Which are the areas you would consider most important for you to enable such collective negotiations?

Response from Open Society European Policy Institute

We support the points raised by one of our partner organisations, Worker Info Exchange (<https://workerinfoexchange.org/>):

1. Legal framework at EU and national level.
2. Regional and City Transport authorities must link together the problems of worker rights, poverty and urban congestion. License to operate must be at stake.
3. Data trusts must be established by unfettered access to GDPR rights. This will bring transparency to pay, utilisation and urban community impact.

We question the titling of this section as 'Self-employed Individuals and Platforms', as this feeds into the problem of misclassification. The title of the section presupposes that gig workers are legally self-employed, when in fact most jurisdictions are now ruling that an employment relationship exists.

## VI. WHAT GOVERNANCE FOR REINFORCING THE SINGLE MARKET FOR DIGITAL SERVICES?

The EU's Single Market offers a rich potential for digital services to scale, including for innovative European companies. Today there is a certain degree of legal fragmentation in the Single Market. One of the main objectives for the Digital Services Act will be to enhance the innovation opportunities and '*deepen the Single Market for Digital Services*'.

This section of the consultation intends to collect evidence and views on the current state of the single market and on steps for further improvements for a competitive and vibrant Single market for digital services. This module also inquires about the relative impact of the COVID-19 crisis on digital services in the Union.

It then focuses on the appropriate governance and oversight over digital services across the EU and means to enhance the cooperation across authorities for an effective supervision of services and for the equal protection of all citizens across the single market. It also inquires about specific cooperation arrangements such as in the case of consumer protection authorities across the Single Market, or the regulatory oversight and cooperation mechanisms among media regulators. This section is not intended to focus on the enforcement of GDPR provisions.

### GOVERNANCE OF DIGITAL SERVICES AND ASPECTS OF ENFORCEMENT

The 'country of origin' principle is the cornerstone of the Single Market for digital services. It ensures that digital innovators, including start-ups and SMEs, have one set of rules to follow (that of their home country), rather than 27 different rules.

This is an important precondition for services to be able to scale up quickly and offer their services across borders. In the aftermath of the COVID-19 outbreak and effective recovery strategy, more than ever, a strong Single Market is needed to boost the European economy and to restart economic activities in the EU.

At the same time, enforcement of rules is key; the protection of all EU citizens regardless of their place of residence, will be in the centre of the Digital Services Act.

The current system of cooperation between Member States foresees that the Member State where a provider of a digital service is established has the duty to supervise the services provided and to ensure that all EU citizens are protected. A cooperation mechanism for cross-border cases is established in the E-Commerce Directive.

**Q61.** Based on your own experience, how would you assess the cooperation in the Single Market between authorities entrusted to supervise digital services?

Response from Open Society European Policy Institute

Over two years after the entry into force of the General Data Protection Regulation (GDPR), one of the EU's regulatory cornerstones for the digital economy, it has become abundantly clear that the weakest element of the EU's regulatory approach to the digital economy is the enforcement of its rules. The EU should address this fundamental deficiency of its regulatory architecture as a matter of top priority.

Traditionally, the EU has regulated different sectors of the economy through separate legal frameworks, each of them with their own supervision and enforcement architecture on top. Increasingly, developments in the market, and in particular the digital economy, significantly challenge this regulatory model. The multitude of legal frameworks applicable and the regulatory authorities in charge of enforcing them that come into play when looking into digital platforms requires a degree of cooperation that is unfortunately insufficient. In practice, this has meant that over the past decades, the EU has come up with many good rules for the digital economy to protect users and their fundamental rights and competitiveness in the market, but the sheer complexity of the enforcement structure and the lack of cooperation mechanisms has meant that many of these rules remain unenforced.

Numerous types of regulatory authorities, and their corresponding European networks, come into play when dealing with digital platforms. National Competition Authorities (NCAs), networked through the European Competition Network (ECN), are in charge of enforcing competition law. National Regulatory Authorities (NRAs), networked through the Body of European Regulators of Electronic Communications (BEREC), are in charge of enforcing rules for electronic communications, some of which also apply to digital platforms. Consumer Protection Agencies (CPAs), networked through the Consumer Protection Cooperation Network (CPC), are in charge of looking after consumer law, which fully applies online. Data Protection Authorities (DPAs), networked through the European Data Protection Board (EDPB), are in charge of enforcing data protection law. Audiovisual and media authorities, networked through the European Regulators' Group for Audiovisual Media Services (ERGA), are in charge of enforcing audiovisual media legislation, also applicable to the relevant online platforms. Market surveillance authorities are in charge of ensuring that products traded inside the EU internal market comply with safety requirements. Cybersecurity law also applies to many digital platforms and is enforced by the European Union Agency for Network and Information Security (ENISA).

By and large, these networks of regulatory authorities do not have the necessary means (or obligations) to ensure they cooperate efficiently and enforce their respective legal frameworks effectively.

Absent formal structures for regulatory cooperation, these networks of authorities have begun cooperating informally. Initiatives such as the Digital Clearinghouse, partially funded by Open Society Foundations, try to bridge that gap by providing a platform through which different regulatory authorities, as well as policy makers, stakeholders, and researchers, can discuss and exchange best practices.

In other sectors such as in energy, initiatives like the Partnership for the Enforcement of European Rights (PEER) aim to connect energy regulators with consumer protection authorities, telecom regulators, and ENISA<sup>24</sup>.

While these initiatives are most welcome and necessary as first steps, the EU needs to be much more ambitious. A dedicated political strategy is urgently necessary to identify the necessary mechanisms to interconnect the different regulatory networks and legal frameworks.

**Q62.** What governance arrangements would lead to an effective system for supervising and enforcing rules on online platforms in the EU in particular as regards the intermediation of third-party goods, services and content (See also Chapter 1 of the consultation)?

Please rate, on a scale of 1 (not at all important) to 5 (very important), each of the following elements.

	1 (NOT AT ALL IMPORTANT)	2	3 (NEUTRAL)	4	5 (VERY IMPORTANT)	I DON'T KNOW / NO ANSWER
1. Clearly assigned competent national authorities or bodies as established by Member States for supervising the systems put in place by online platforms					X	
2. Cooperation mechanism within Member States across different competent authorities responsible for the systematic supervision of online platforms and sectorial issues (e.g. consumer protection, market surveillance, data protection, media regulators, anti-discrimination agencies, equality bodies, law enforcement authorities etc.)					X	

24 <https://www.ceer.eu/peer>

	1 (NOT AT ALL IMPORTANT)	2	3 (NEUTRAL)	4	5 (VERY IMPORTANT)	I DON'T KNOW / NO ANSWER
3. Cooperation mechanism with swift procedures and assistance across national competent authorities across Member States					X	
4. Coordination and technical assistance at EU level					X	
5. An EU-level authority			X			
6. Cooperation schemes with third parties such as civil society organisations and academics for specific inquiries and oversight						
7. Other: please specify in the text box below						

**Q63.** Response from Open Society European Policy Institute

It is important to make sure that competences are distributed and assigned among different regulators clearly and efficiently. Numerous inefficient situations exist already where the way EU rules have been implemented nationally do not allow for efficient cross-border enforcement of rules. For example, Member States sometimes interpret EU rules loosely and give powers to departments in their national ministries when such powers are intended to be exercised by truly independent agencies. Those non-independent entities are not part of the relevant EU-wide regulatory network, creating therefore a geographical enforcement gap in the system.

It is therefore important for any new rules on digital platforms that the EU adopts to include very clear mandates for Member States to establish the regulatory mechanisms necessary to enable efficient cross-border enforcement. EU Institutions must prioritise questions of efficiency of enforcement over recurring debates of national sovereignty or other domestic political considerations.

Other times, the main challenge with enforcing EU rules applicable in the digital economy are the lack of financial, human and technical resources provided to these authorities.

As argued above, it is essential that a cooperation mechanism connecting regulators within Member States, and across borders through the relevant networks, be established as a matter of priority.

Any new enforcement authority created by the Digital Services Act must be intertwined with existing regulatory networks at European level and the relevant individual authorities at national level. Such an authority must be carefully designed to ensure its independence both from national Governments and EU institutions, as well as from the market players it is intended to monitor and oversee.

Involving civil society and academics in the regulatory process is also important. Often, it will be experts in the field and representatives of minority or racialised groups the ones that will be best prepared to defend their interests. This is of utmost importance particularly when speaking about certain types of digital platforms where these groups of people are all too often the ones most negatively impacted by online content which requires careful debate and analysis when contested.

**Q64.** In your view, is there a need to ensure similar supervision of digital services established outside of the EU that provide their services to EU users?

- Yes, if they intermediate a certain volume of content, goods and services provided in the EU
- Yes, if they have a significant number of users in the EU
- No
- Other
- I don't know

**Q65.** Response from Open Society European Policy Institute

Important pieces of EU law already apply to companies that are not based in the EU. For example, companies that target their products and services at European consumers must comply with EU consumer law, and companies that collect and/or process personal data of people in the EU must comply with the General Data Protection Regulation.

A similar principle should apply regarding rules in the Digital Services Act. As the internet is to a certain extent borderless, this will be a necessary first step for the EU to ensure that the fundamental rights and democratic principles it is trying to enforce within its borders are respected.

It could also be a helpful regulatory technique if it spilled over to other parts of the world that need to take a more protective stance towards fundamental rights and democratic principles.

**Q66.** 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?

Designing an efficient coordination mechanism is a highly complex matter that will require proper analysis and determined action. The European Commission should urgently develop an ambitious strategy to gather the necessary political agreement from national governments, political parties and MEPs so that all agree on fast-tracking an architectural solution to the enforcement gap problem.

In parallel, the European Commission should deploy a policy-making process designed to explore different responses to this question, involving relevant stakeholders, in particular from the regulators and authorities themselves and from the civil society organisations that struggle to keep providers of digital services accountable due to the sheer complexity of the enforcement field in the EU.

**Q67.** Would the current system need to be strengthened? If yes, which additional tasks be useful to ensure a more effective enforcement of audiovisual content rules?

Please assess from 1 (least beneficial) – 5 (most beneficial). You can assign the same number to the same actions should you consider them as being equally important.

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



