European Commission Digital Services Act package

Global Partners Digital submission

September 2020

About Global Partners Digital

Global Partners Digital is a social purpose company dedicated to fostering a digital environment underpinned by human rights.

Introduction

In this submission response from Global Partners Digital and Ranking Digital Rights, we would like to take this opportunity to provide our thoughts and respond to the Digital Services Act public consultation. We recognise the desire of the European Commission to propose new and revised rules to deepen the Single Market for Digital Services, by increasing and harmonising the responsibilities of online platforms and information service providers and reinforce the oversight over platforms' content policies in the EU. We also recognise the desire 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.

We are, however, concerned that certain aspects of a new or revised regulatory framework may pose risks to individuals' rights to freedom of expression and privacy, and could be inconsistent with EU member states international human rights obligations and the European Convention on Human Rights (ECHR).

Framework for Response to Consultation

Our responses to the questions posed in the consultation are based on international human rights law, primarily the International Covenant of Civil and Political Rights (ICCPR), and the ECHR. The most relevant human rights impacted by a new or revised framework are the rights to freedom of expression and privacy. Article 19 of the ICCPR guarantees the right to freedom of expression, including the right to receive and impart information and ideas of all kinds regardless of frontiers. Article 17 of the ICCPR guarantees the right to privacy and provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence". The rights to freedom of expression and privacy are also protected in the European Convention on Human Rights (Articles 10 and 8 respectively) and the EU Charter of Fundamental Rights (Articles 11 and 7 respectively).

As well-established under international human rights law, the ECHR and the EU Charter of Fundamental Rights, restrictions on the rights to freedom of expression and privacy are only permissible when they can be justified. In order to be justified, a restriction must meet a three-part test, namely that: (i) it is provided by law; (ii) it pursues a legitimate aim; and (iii) it is necessary and proportionate, which requires that the restriction be the least restrictive means required to achieve the purported aim.

It is important to remember that EU member states have an obligation to ensure that these rights are not unjustifiably restricted both in relation to restrictions which stem from the actions of the state itself, as well as those caused by third parties, such as private companies. As such, it makes no difference from the perspective of the individual affected whether any restrictions are imposed and enforced directly by the state (e.g. through creating criminal offences which are enforced by the police and the courts) or through third parties, particularly when the third party is acting in order to comply with legal obligations.

With respect to the actions of private companies specifically, the United Nations Guiding Principles on Business and Human Rights (UNGPs) makes clear that a state's international human rights obligations include establishing a legal and policy framework which enables and supports businesses to respect human rights. Principle 3 notes that this general obligation includes ensuring "that (...) laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights".

Given the impact that online platforms have upon the enjoyment and exercise of the rights to freedom of expression and privacy, EU member states have a clear obligation to ensure that these rights are respected by these platforms. This includes ensuring that legislation and other measures do not constrain online platforms' ability to respect the right to freedom of expression or privacy themselves, nor should they directly or indirectly constitute a restriction on the enjoyment and exercise of those rights by those that use such platforms.

Our responses to the questions posed in the consultation are based on these frameworks. Given the limited existing interpretation and case-law of these frameworks, we also make reference, as appropriate, to Recommendation CM/Rec(2018)2 of the Council of Europe's Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Recommendation CM/Rec(2018)2),[1] and relevant commentary from the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (the UN Special Rapporteur). These guidelines and commentaries provide detail on the obligations of states with respect to the protection and promotion of human rights in the digital environment, with a particular focus on any legal frameworks that apply to internet intermediaries.

Though not a framework for the purpose of our analysis, we note that various EU member states have, through their membership of the Freedom Online Coalition, signed up to a number of commitments which are relevant to the subject. These includes commitments made in the "Recommendations for Freedom Online, Adopted in Tallinn, Estonia on April 28, 2014 by Ministers of the Freedom Online Coalition":

> "We, the members of the Freedom Online Coalition

[1] Council of Europe, Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, 7 March 2018.

> 4. Dedicate ourselves, in conducting our own activities, to respect our human rights obligations, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency, and call upon others to do the same,
>
> (…)
>
> 6. Call upon governments worldwide to promote transparency and independent, effective domestic oversight related to electronic surveillance, use of content take-down notices, limitations or restrictions on online content or user access and other similar measures, while committing ourselves to do the same".[2]

More recent commitments were made in the Freedom Online Coalition's "Joint Statement on Internet Censorship":

> "In 2017, the world witnessed state-sponsored Internet censorship in various forms: states have manipulated and suppressed online expression protected by international law, have subjected users to arbitrary or unlawful surveillance, have used liability laws to force ICT companies to self-censor expression protected by international law, have disrupted networks to deny users access to information, and have employed elaborate technical measures to maintain their online censorship capabilities. Further unlawful efforts included state censorship in private messaging apps and systematic bans of news websites and social media. Likewise certain states have introduced or implemented laws which permit executive authorities to limit content, on the Internet broadly and without appropriate procedural safeguards. Individuals who may face multiple and intersecting forms of discrimination, including women and girls, often faced disproportionate levels of censorship and punishment.
>
> (...)
>
> The FOC firmly believes in the value of free and informed political debate, offline and online, and its positive effects on long term political stability. The Coalition calls on governments, the private sector, international organizations, civil society, and Internet stakeholders to work together toward a shared approach - firmly grounded in respect for international human rights law - that aims to evaluate, respond to, and if necessary, remedy state-sponsored efforts to restrict, moderate, or manipulate online content, and that calls for greater transparency of private Internet companies' mediation, automation, and remedial policies."[3]

[2] Recommendations for Freedom Online, Adopted in Tallinn, Estonia on April 28, 2014 by Ministers of the Freedom Online Coalition, available at: https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf.
[3] The Freedom Online Coalition, Joint Statement on Internet Censorship, available at: https://freedomonlinecoalition.com/wp-content/uploads/2018/05/FOC-Joint-Statement-on-Internet-Censorship-0518.pdf.

I. How to effectively keep users safer online?

1. Main issues and experiences

B. Transparency

18. How has the dissemination of illegal content changed since the outbreak of COVID-19? Please explain. (3000 character(s) maximum)

Since the outbreak of COVID-19, there has been an increase in certain types of illegal content as individuals around the world spend more time online.[4] This includes child sexual abuse imagery and certain forms of illegal hate speech. This has put additional pressure on states and companies to take steps to ensure that the online environment is safe. Unfortunately, many of the steps taken both before and since the outbreak pose risks to human rights, particularly the rights to freedom of expression and privacy.

19. What good practices can you point to in handling the dissemination of illegal content online since the outbreak of COVID-19? (3000 character(s) maximum)

There are, unfortunately, few good practices to which we can point in the handling of dissemination of illegal content online since the outbreak of COVID-19. Instead, many of the steps that have been taken have raise concerns over the risks that they pose to human rights, particularly the rights to freedom of expression and privacy.

- Some governments, such as those in Hungary and Russia, have responded to the pandemic through censorship and illegitimately restricting individuals freedom of expression.[5] Other governments, even those with legitimate intentions, have utilised existing laws or created new criminal laws to combat illegal content online that do not adhere to the principles of legality, proportionality and necessity.

- Companies have continued to fail to be transparent about their policies and actions, particularly in the enforcement of their terms of service or the adherence of their content moderation decisions to relevant international human rights standards. One example is Facebook, whose recent Civil Rights Audit faulted the social media platform for allowing hate speech to thrive and acknowledged the additional challenges facing the platform to address illegal content in light of COVID-19.[6]

Most practices employed by state and private actors to tackle the dissemination of illegal content online were in place before the outbreak of COVID-19. Many of these existing efforts

---

[4] See, for example, UNICEF, 'COVID-19 and its Implications for Protecting Children Online', April 2020, available at: https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf; and UN DGC, 'United Nations Guidance Note on Addressing and Countering COVID-19 Related Hate Speech', 11 May, 2020, available at: https://www.un.org/en/genocideprevention/documents/Guidance%20on%20COVID-19%20related%20Hate%20Speech.pdf

[5] See, for example, S. Walker, 'Hungarian Journalists Fear Coronavirus law May be used to Jail Them', The Guardian, 3 April 2020, available at: https://www.theguardian.com/world/2020/apr/03/hungarian-journalists-fear-coronavirus-law-may-be-used-to-jail-them, and D. Litvinova, 'Fake News or the Truth? Russia Cracks Down on Virus Postings' AP News, 1 April 2020, available at: https://apnews.com/dbbf02a747b11d8ffe3b07d5e33ff129

[6] Facebook's Civil Rights Audit - Final Report, 8 July 2020, available at: https://about.fb.com/wp-content/uploads/2020/07/Civil-Rights-Audit-Final-Report.pdf

were previously criticised as being insufficient to fully address the issue, which has become more clear during the pandemic. For example, review of potentially illegal content is now increasingly done through automated processes as it has become increasingly difficult for humans to provide additional oversight. This is due to an increase in content itself and the current physical limitations of human reviewers. Ideally, good practice would involve states and private actors working together to respond to the proliferation of illegal content during the crisis while still protecting human rights online.

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

1. In your experience, are children adequately protected online from harmful behaviour, such as grooming and bullying, or inappropriate content? (3000 character(s) maximum)

Children continue to face risks from certain forms of harmful behaviour online, such as grooming and exploitation.[7] It is, however, essential, that measures taken to protect children from harmful behaviour do not create risks to human rights, including children's human rights, which include the rights to freedom of expression and privacy.

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

	Fully agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Fully disagree	I don't know/ No reply
Online platforms can easily be manipulated by foreign governments or other coordinated groups to spread divisive messages		x				
To protect freedom of expression online, diverse voices should be heard	x					
Disinformation is spread by manipulating algorithmic processes on online platforms		x				
Online platforms can be trusted that their internal practices sufficiently guarantee democratic integrity, pluralism, non-					x	

[7] EUROPOL, 'Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse during Covid-19 Pandemic' 19 June 2020, available at: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic

discrimination, tolerance, justice, solidarity and gender equality.						

3. Please explain. (3000 character(s) maximum)

We recognise the challenges and threats posed by disinformation through social media and communications platforms, often causing very real harms. We agree that online platforms can be manipulated by foreign governments or other coordinated groups to spread divisive messages, which may infringe on individuals' right to health, right to free and fair elections, or rights to equality and non-discrimination. We are particularly concerned, however, with the actions that some states have taken to tackle the issue of disinformation through regulatory responses.

Most forms of legislation prohibiting false or misleading information are loosely-defined in their scope, meaning that authorities could interpret them as giving them power to restrict a wide range of speech from diverse voices; and they pursue aims which would not be considered legitimate according to international human rights standards. These laws also carry penalties which can be disproportionate and result in a chilling effect on freedom of expression.

Policymakers should consider alternate means of tackling disinformation, such as through improving digital literacy, increasing transparency by social media platforms on algorithmic decision making, or pursuing voluntary arrangements before resorting to regulation. Many of these initiatives are currently being pursued by the EU, and the success of failure of such efforts should inform any new or revised obligations on platforms.

4. In your personal experience, how has the spread of harmful (but not illegal) activities online changed since the outbreak of COVID-19? Please explain. (3000 character(s) maximum)

The outbreak of COVID-19 has seen an increase in certain forms of harmful (but not illegal) activities and content online, such as disinformation/misinformation relating to COVID-19, which has prompted the World Health Organisation (WHO) to declare an "infodemic".[8] In addition, there has been a rise in hate speech (that which does not reach the threshold of illegality and that which does) against certain groups.[9]

5. What good practices can you point to in tackling such harmful activities since the outbreak of COVID-19? (3000 character(s) maximum)

There are some good practices undertaken by states, international organisations, and companies in tackling such harmful activities since the outbreak of COVID-19.

- Both the UK and the EU have established partnerships with international organisations, such as the WHO, to counter disinformation/misinformation about COVID-19 through awareness-raising campaigns. Certain EU member states' health ministries have also

[8] OECD, 'Combatting COVID-19 Disinformation on Online Platforms' 3 July 2020, available at: http://www.oecd.org/coronavirus/policy-responses/combatting-covid-19-disinformation-on-online-platforms-d854ec48/

[9] C. Timberg and A. Chiu, 'As the Coronavirus Spread, so does Online Racism Targeting Asians, New Research Shows' The Washington Post, 8 April 2020, available at: https://www.washingtonpost.com/technology/2020/04/08/coronavirus-spreads-so-does-online-racism-targeting-asians-new-research-shows/.

been actively working to combat harmful pieces of COVID-19 related misinformation, as seen in France.

- Platforms such as Facebook have committed themselves to prioritising content from authoritative sources, and cooperating with fact-checkers and health authorities to flag and remove COVID-19 related disinformation/misinformation. Platforms have agreed to work together on this front as well. However, the results of these efforts have been criticised, particularly because of platforms' enhanced reliance on automated content moderation and overall lack of transparency.

D. Experiences and data on erroneous removals

1. Are you aware of evidence on the scale and impact of erroneous removals of content, goods, services, or banning of accounts online? Are there particular experiences you could share? (5000 character(s) maximum)

The scale of erroneous removals of content is likely to increase as platforms continue to resort to automated processes for content moderation. It has been widely observed that AI is at a very nascent stage when it comes to analysing speech, and can only accurately identify a very small number of categories of speech which don't require an assessment of context or other nuances.[10] AI has had some success in relation to images, as opposed to speech, with its most successful application being to identify copies of images already identified by humans as constituting child sexual abuse and exploitation.

However, using AI to identify new images of potentially illegal or harmful content or activity is far more difficult. The example of Tumblr which used automated processes to identify content which breaches its standards on "adult content", with large swathes of innocent content being flagged, shows how easily reliance on automated processes can lead to over-removal of content.[11] Over-removal is even more likely when it comes to speech, given that context is even more relevant. As such, there are particular risks to freedom of expression and the erroneous removal of permissible content, which stem from the use of automated processes in order to determine whether content is illegal or harmful.

[10] See, for example, Center for Democracy & Technology, "Mixed Messages? The Limits of Automated Social Media Content Analysis", 28 November 2017, available at: https://cdt.org/insight/mixedmessages-the-limits-ofautomatedsocial-media-content-analysis.

[11] See, for example, Montgomery, S. J., "Here's Some of the Random Content Tumblr Is Flagging for Its No-Porn Policy", complex.com, 5 December 2018, available at: https://www.complex.com/life/2018/12/contenttumblr-is-flagging-for-no-adult-content-policy/; Romano. A., "Tumblr is banning adult content. It's about so much more than porn", Vox, 17 December 2018, available at: https://www.vox.com/2018/12/4/18124120/tumblrporn-adult-content-ban-user-backlash.

2. Clarifying responsibilities for online platforms and other digital services

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

	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)	Yes, only by larger online platforms	Yes, only platforms at particular risk of exposure to illegal activities by their users	Such measures should not be required by law
Maintain an effective 'notice and action' system for reporting illegal goods or content			x	
Maintain a system for assessing the risk of exposure to illegal goods or content			x	
Have content moderation teams, appropriately trained and resourced			x	
Systematically respond to requests from law enforcement authorities			x	
Cooperate with national authorities and law enforcement, in accordance with clear procedures			x	
Cooperate with trusted organisations with proven expertise that can report illegal activities for fast analysis ('trusted flaggers')				x
Detect illegal content, goods or services				x
In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law	x			
Request professional users to identify themselves			x	

clearly ('know your customer' policy)				
Provide technical means allowing professional users to comply with their obligations (e.g. enable them to publish on the platform the pre-contractual information consumers need to receive in accordance with applicable consumer law)			x	
Inform consumers when they become aware of product recalls or sales of illegal goods				
Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities			x	
Be transparent about their content policies, measures and their effects			x	
Maintain an effective 'counter-notice' system for users whose goods or content is removed to dispute erroneous decisions			x	
Other. Please specify				

2. Please elaborate, if you wish to further explain your choices. (5000 character(s) maximum)

Responsibilities (i.e. legal obligations) imposed on online platforms should not be overly prescriptive, and should only apply where there is sufficiently strong evidence of a likelihood of illegal or harmful activity.

Different forms of illegal or harmful content will require distinct public policy approaches. A single regulatory response which establishes responsibilities across all online platforms is unlikely to effectively tackle the very different considerations that each form of illegal or harmful content requires, and obligations on platforms should reflect this narrowly tailored, proportionate and nuanced approach. In our answers below, we set out more detail on what measures might be appropriate and proportionate for online platforms in relation to both illegal and harmful activities and content.

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

- **Precise location: e.g. URL**
- **Precise reason why the activity is considered illegal**
- **Description of the activity**
- **Identity of the person or organisation sending the notification. Please explain under what conditions such information is necessary:**
- Other, please specify

4. Please explain (3000 character(s) maximum)

While we generally agree that the information identified in question 3 could be necessary and sufficient in some circumstances, we believe that the information necessary and sufficient for users and third parties will ultimately depend on the specific service and particular online content or activity in question. There should always be a sufficient degree of friction in the notification process to mitigate the risk of unjustified complaints. Accessibility must be balanced with the need to protect users from false reports, as individuals may allege illegal or prohibited content as a means of shutting down legitimate expression.

5. How should the reappearance of illegal content, goods or services be addressed, in your view? What approaches are effective and proportionate? (5000 character(s) maximum)

The reappearance of illegal content should be addressed based on the specific type of illegal content, and the surrounding circumstances. Only a very small number of types of illegal content will always be illegal, regardless of context, with one example being child sexual abuse imagery. Automated tools such as hashing databases could be appropriately used in these cases. However, the legality or many other types of content depends on context. A video of a terrorist attack, for example, may be illegal glorification of terrorism in some circumstances and legal academic research in another. The nuanced and context-specific nature of this determination requires human oversight, cooperation among platforms, and should not be left to automatic processes alone.

6. Where automated tools are used to detect illegal content, goods or services, what opportunities and risks does their use present as regards different types of illegal activities and the particularities of the different types of tools? (3000 character(s) maximum)

A range of automated tools exist for the detection of illegal content or activities. Hash databases are useful for the identification of identical content or pre-existing images. This type of detection usually requires an identical match and presents few risks. Other types of tools or processes are simply based on the likelihood of a match. While AI can estimate likelihood, there are concerns that platforms may remove content with lower levels of likelihood, which risks erroneous removals of legitimate expression. Companies should be encouraged to be transparent as to what automated tools are utilised to detect illegal content and activities.

7. How should the spread of illegal goods, services or content across multiple platforms and services be addressed? Are there specific provisions necessary for addressing risks brought by:

a. Digital services established outside of the Union?

b. Sellers established outside of the Union, who reach EU consumers through online platforms? (3000 character(s) maximum)

In addressing the spread of illegal goods, services or content across multiple platforms, including those outside of the EU, we would encourage a framework which applies to companies based outside of the EU when offering their services within the EU, but which also ensures that this would not require the global removal of content (even illegal content) outside the EU.

8. What would be appropriate and proportionate measures for digital services acting as online intermediaries, other than online platforms, to 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.? (5000 character(s) maximum)

We recognise the difficulty in determining appropriate and proportionate measures for digital services acting as online intermediaries other than online platforms. However, we caution against responsibilities being applied to online intermediaries without there being any evidence of harm being caused or facilitated by their services. Their inclusion in the scope of new or revised legislation would be neither proportionate nor appropriate without such evidence. The EU should consider these measures in the most narrow way possible, and only apply them where evidence exists of their services causing or facilitating harm.

9. What should be the 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? (5000 character(s) maximum)

We caution against responsibilities being imposed on other entities, such as authorities or interested third-parties such as civil society organisations. We do, however, encourage oversight mechanisms to be established for civil society organisations to raise human rights concerns or monitor the effective implementation or compliance with regulations.

10. What would be, in your view, appropriate and proportionate measures for online platforms to take in relation to activities or content which might cause harm but are not necessarily illegal? (5000 character(s) maximum)

While there are potentially many measures that online platforms could take in relation to activities or content which might cause harm but are not necessarily illegal, we believe that the most appropriate and proportionate measures relate directly to (i) ensuring clarity over their terms of service and (ii) transparency over their enforcement and the use of algorithms.

- Online platforms could be required to provide clarity over their terms of service which relate to content which is harmful, but not necessarily illegal. Where online platforms prohibit or moderate such forms of content, they could be required to ensure that this is clear to users, and that they enforce those terms of service fairly and consistently.
- Online platforms could also be required to provide greater transparency on the enforcement of these terms of service, including any use of algorithms in identifying or moderating content which is harmful, but not necessarily illegal. Appropriate transparency reporting requirements should not, however, incentivise companies to act in a way that presents risks to freedom of expression or privacy.

There is a clear benefit in this approach from a human rights perspective as it makes clear what forms of content a platform will remove or restrict, allowing for comparison with the justified limitations on freedom of expression. It further enables users to know, with a reasonable degree of confidence, under what circumstances content they wish to make available will be removed or restricted, ensuring transparency and certainty. They also provide authorities, or oversight bodies, with an opportunity to assess compliance with international human rights standards.

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

	1	2	3	4	5	I don't know / No answer
Transparently inform consumers about political advertising and sponsored content, in particular during election periods					x	
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with user complaints					x	
Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives					x	
Transparency tools and secure access to platform data for trusted researchers in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it					x	
Transparency tools and secure access to platform data for authorities in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it				x		
Adapted risk assessments and mitigation strategies undertaken by online platforms					x	
Ensure effective access and visibility of a variety of authentic and professional journalistic sources					x	
Auditing systems for platform actions and risk assessments					x	
Regulatory oversight and auditing competence over platforms' actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on the manipulation and amplification of disinformation					x	
Other (please specify)					x	

13. Please specify (3000 character(s) maximum)

Tackling disinformation and misinformation online requires a multi-pronged approach, which may require new or revised measures for online platforms. In addition to our answers above on potential measures for addressing harmful but not illegal content online, we would like to expand on a few of the measures here.

- As noted above, it may be appropriate to require online platforms companies provide clarity over their terms of service which relate to content which is harmful, but not necessarily illegal. Whether this includes disinformation or misinformation should be left to the online platforms to determine, however if they do introduce terms of service relating to these types of content, they could be required to ensure that this is clear to users, and that they have mechanisms in place to ensure that those terms of service are enforced as fairly and consistently as possible.

- It may also be appropriate for policymakers to require certain companies to develop transparency reports about their actions taken on disinformation, misinformation (where prohibited or moderated under their terms of service) and political advertising, providing both users and an appropriate oversight body with adequate information, particularly around elections and during public health crises. These should cover the use of algorithms in identifying or moderating content. Under no circumstances should states simply shift the responsibility to tackle disinformation to platforms, or require them to make legal determinations.

- While we do not recommend this as a mandatory measure, we would encourage companies to ensure effective access and visibility of authoritative sources where appropriate. For larger platforms, we recommend that this go beyond fact checking initiatives, but involve further efforts to educate and build the digital literacy of users to recognise disinformation for themselves. This could be achieved, in part, by providing notices to users previously exposed to misleading content. And it should be accomplished through consultation and collaboration with relevant civil society organisations, fact checking initiatives, and local experts.

14. In special cases, where crises emerge and involve systemic threats to society, such as a health pandemic, and fast-spread of illegal and harmful activities online, what are, in your view, the appropriate cooperation mechanisms between digital services and authorities? (3000 character(s) maximum)

In these special cases, there may be some tools or mechanisms that could be utilised to address the fast-spread of illegal and harmful activities online.

- One of these cooperation mechanisms would involve a crisis protocol. Such protocols have been developed, or are currently being developed across the globe: EU Crisis Protocol or Christchurch Call Crisis Protocol. These protocols must be proportionate in their design and application to avoid risks to freedom of expression.
- Other quick-response initiatives, such as those developed at the G7, NATO, or EU level should be encouraged to work with other international processes to provide a unified front against systemic threats.

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

	1	2	3	4	5	I don't know / No answer
High standards of transparency on their terms of service and removal decisions					x	
Diligence in assessing the content notified to them for removal or blocking					x	
Maintaining an effective complaint and redress mechanism					x	
Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended					x	
High accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts					x	
Enabling third party insight – e.g. by academics – of main content moderation systems					x	
Other. Please specify					x	

16. Please explain. (3000 character(s) maximum)

In addition to the measures mentioned here, any additional obligations on service providers should be considered alongside their potential impacts on freedom of expression and privacy. Ongoing stakeholder engagement would be particularly helpful to mitigate risks to these rights. In addition to academics, civil society organisations - particularly digital rights groups, would be well placed to advise on what measures may promote or create risks to users freedom of expression. National human rights bodies within EU member states would also be well suited to provide advice and monitoring of activities.

17. Are there other concerns and mechanisms to address risks to other fundamental rights such as freedom of assembly, non-discrimination, gender equality, freedom to conduct a business, or rights of the child? How could these be addressed? (5000 character(s) maximum)

We believe that the full array of rights must be considered here, but are particularly concerned about children's right to freedom of expression. We recommend that any new framework be developed while considering minors' right to freedom of expression as provided for in Article 13 of the Convention on the Rights of the Child. We would also like to stress that any obligations

should consider the potential impact on the right to privacy, specifically in regard to encryption and private communication channels.

18. In your view, what information should online platforms make available in relation to their policy and measures taken with regard to content and goods offered by their users? Please elaborate, with regard to the identification of illegal content and goods, removal, blocking or demotion of content or goods offered, complaints mechanisms and reinstatement, the format and frequency of such information, and who can access the information. (5000 character(s) maximum)

Online platforms should, at a minimum: (i) inform affected users of content that has been flagged for removal, restriction or moderation; (ii) create an opportunity for that user to be able to input into the moderation process; and (iii) provide an appeal mechanisms for affected users to challenge decisions. This should be dealt with in a timely manner, which takes into account the particular circumstances, platform, users and content in question.

19. What type of information should be shared with users and/or competent authorities and other third parties such as trusted researchers with regard to the use of automated systems used by online platforms to detect, remove and/or block illegal content, goods, or user accounts? (5000 character(s) maximum)

Due to a lack of transparency on how algorithms and other automated systems detect, remove, and/or block illegal content, goods, or user accounts, we would recommend that the maximum amount of information be shared with competent authorities or trusted researchers through a data trust model, with researchers given the ability to independently assess and report findings. It would also be beneficial to provide users with accurate information on when algorithms and other automated processes are used, and what specific data goes into these algorithms and processes, and the level of accuracy observed. Appeal mechanisms should also be provided to users with an opportunity to challenge decisions as appropriate.

20. In your view, what measures are necessary with regard to algorithmic recommender systems used by online platforms? (5000 character(s) maximum)

Measures should be devised so that users understand what types of controls or algorithms are in place, including the data points used to make recommendations. Moreover, users should have a say in whether these algorithmic recommender systems are applied, and have the option to turn them off, or instead only have them base recommendations on specific data points agreed to by the user.

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

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

22. Please explain. What would be the benefits? What would be concerns for companies, consumers or other third parties? (5000 character(s) maximum)

Yes, there is a need for enhanced data sharing between online platforms and authorities within the boundaries set by the GDPR. However, further guidance is needed as the GDPR is a general framework that doesn't set out specific rules and expectations on how this would apply to sharing data on accuracy, the use of specific data points, or what this means for informing users.

23. What types of sanctions would be effective, dissuasive and proportionate for online platforms which systematically fail to comply with their obligations (See also the last module of the consultation)?

Heavy or disproportionate sanctions will skew incentives and exacerbate risks to freedom of expression. If an online platform is making decisions as to whether to remove, restrict or otherwise moderate content or not on the basis that it might potentially be illegal or harmful, there will be a strong incentive to 'play it safe' and simply do so rather than risk sanction. The heavier the potential sanction, the greater the incentive.

Noting this risk, Recommendation CM/Rec(2018)2 states that "[s]tate authorities should ensure that the sanctions they impose on intermediaries for non-compliance with regulatory frameworks are proportionate because disproportionate sanctions are likely to lead to the restriction of lawful content and to have a chilling effect on the right to freedom of expression".

Instead, proportionate sanctions might include (i) serving a notice to a company that is alleged to have breached their obligations, and set a timeframe to respond with a plan to rectify the issue; (ii) requiring additional information from the company regarding the alleged failure to comply with obligations; and (iii) publishing public notices about the proven failure of the company to comply with obligations. Civil sanctions would only be appropriate after these had been exhausted, and the proportionality of such fines would ultimately depend on the specifics of the offence.

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

2. The liability regime for online intermediaries is primarily established in the E-Commerce Directive, which distinguishes between different types of services: so called 'mere conduits', 'caching services', and 'hosting services'. In your understanding, are these categories sufficiently clear and complete for characterising and regulating today's digital intermediary services? Please explain. (5000 character(s) maximum)

There may be a benefit to revising the different types of services within scope of any new regulation to ensure that the categorisation is fit for purpose, is clear to stakeholders, and provides sufficient protections to all relevant parts of the ecosystem.

It may be helpful to consider existing proposals, such as those presented to the European Commission DG Communications Networks, Content & Technology by the Institute for

Information Law (IViR) in 2019.[12] This study presented a typology of hosting services in the following categories: (1) storage and distribution; (2) networking, collaborative productive and matchmaking; and (3) selection, search and referencing.

3. Are there aspects that require further legal clarification? (5000 character(s) maximum)

Yes. Further legal clarification is needed over the term "actual knowledge". The E-Commerce Directive does not actually define what is meant by actual knowledge or when a caching provider or hosting provider is "facts or circumstances from which the illegal activity or information is apparent".

A provider should only be considered to have "actual knowledge" when it has been informed by an appropriate body, such as a court, of its determination that a particular instance of activity or piece of information is illegal. The providers should not themselves be required or expected to make determinations of legality. As such, even being aware of activity or information should not in and of itself constitute "actual knowledge" without the provider also being aware of the appropriate body's determination that it is illegal. To provide otherwise would be to expect online platforms with no or limited expertise to make legal determinations, raising serious concerns from a rule of law perspective, and risking freedom of expression as there will be a strong incentive to "play it safe" and avoid sanctions by simply removing content.

4. Does the current legal framework dis-incentivize service providers to take proactive measures against illegal activities? If yes, please provide your view on how disincentives could be corrected. (5000 character(s) maximum)

Yes. The current legal framework may disincentivise service providers from taking proactive measures against illegal activities in the absence of a Good Samaritan clause.[13] Disincentives could be corrected or reduced through the introduction of such a clause, comparable to Section 230 of the Communications Decency Act in the US. Any such clause should be drafted in a manner so as not to encourage excessive take-downs on the provider's own initiative, or produce other risks to freedom of expression.

We are concerned that the approach suggested in the European Commission's 2017 Communication on Tackling Illegal Content Online does not sufficiently clarify the issue of intermediary liability or (Good Samaritan actions) and should not serve as the basis for a Good Samaritan clause in the Digital Services Act. The Communication suggests that providers would not lose liability from proactive measures as long as they chose to act expeditiously to remove content when they obtain knowledge of illegal activity. Instead, the protection should be extended to any use of proactive measures taken in good faith even when illegal content is missed and no action is taken to remove it.

6. 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. (5000 character(s) maximum)

[12] Directorate-general for Communications Network, Content and technology (European Commission) and Institute for Information Law, 'Hosting Intermediary Services and Illegal Content Online: An Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape Final Report' January 2019, available at: (IViR)https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en/format-PDF
[13] Ibid.

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. (5000 character(s) maximum)

Yes and further clarification is needed as to the parameters for general monitoring obligations as decisions by the CJEU have undermined the protections in the E-Commerce Directive. In *Glawischnig-Piescek v Facebook Ireland Limited*, the court held that the rule against imposing general monitoring obligations did not preclude member states from being able to require hosting platforms to remove illegal user-generated content, or any content that was "identical" or "equivalent".

Not only does this decision undermine the protections in the E-Commerce Directive, it has created risks to freedom of expression. First, it fails to proper clarity over what would constitute "equivalent" content and leaves it to national courts to consider the contours of this term, risking a fragmented approach. Second, it puts the onus on platforms to develop and use automated tools to remove such content. This presents risks as it assumes that automated tools can correctly identify "equivalent" content in varying contexts. In practice, this may lead to the over removal of legitimate content.

More generally, maintaining a prohibition on general monitoring or obligations to seek facts or circumstances of illegal activities is critical to protecting individuals' right to privacy. In the absence of such prohibitions, there is a risk of creating a situation where all content may need to be potentially approved before it is published.