BILETA's Response to the EU's Consultation on the Digital Services Act

Leiser, M.R.; Harbinja, E.; Blakely, M.; Romero, F.R.; Barker, K.; Coozigou, I.

BILETA DSA Response

Part I How to effectively keep users safer online?

Part 1A

Q1 Have you ever come across illegal goods on online platforms (e.g. a counterfeit product, prohibited and restricted goods, protected wildlife, pet trafficking, illegal medicines, misleading offerings of food supplements)?

Yes, several times.

Q3 Please specify.

The number of illegal products has increased since the beginning of the COVID-19 pandemic outbreak. Indeed, due to pandemic responses around the world, many States limited the movement of people and those bought more essential items online. When traditional forms of commerce adapted to the crisis and became new businesses online, they were not always successful in protecting consumers. Given the high demand, many illegal products were medical supplies. Thus, there was a significant number of products which was falsely presented as able to cure or prevent COVID-19 infections or counterfeit facemasks, other protective equipment and testing kits. The COVID-19 crisis has also heightened product safety risks. Recall notices of facemasks that do not adequately filter airborne particles and may expose consumers to risk of infection if not combined with additional protective measures, have been for example recently submitted to the OECD's GlobalRecalls portal, a database for governments to share recall information.

Below are a few examples of COVID-19 scams:

The UK's National Cyber Security Centre (NCSC) said it took down more than 2,000 online coronavirus scams in March alone, which included 471 fake online shops selling fraudulent COVID-19-related items.

Police in France removed 70 fraudulent websites claiming to sell chloroquine in April.

COVID-19-related scams in the USA amounted to approximately US$13.4 million in fraud, from the beginning of January to mid-April this year and have affected more than 18,000 citizens.

A seizure of 3,300 thermometers was reported in Thailand, after being trafficked through three other countries and a report of thermometers which do not conform with EU regulations was also noted in Italy.

Organized criminal groups in the Western Balkans are believed to be involved in money laundering and investing their illicit gains in the production and trafficking of falsified medical products and protective clothing.

There have been COVID-19-related reports of substandard and falsified ventilators in Russia, where a fraud enquiry has begun, as well as in the UK, where ventilators supplied were substandard and potentially dangerous. The supply of substandard ventilators was also reported in Bosnia and Herzegovina.[1]

Q4 N/A
Q5 N/A
Q6 N/A
Q7 N/A
Q8 N/A

Q9 **In your experience, were such goods more easily accessible online since the outbreak of COVID-19?**

Yes, we came across illegal offerings more frequently

Q10 N/A

Q11 **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 that infringes intellectual property rights, consumer law infringements)?**

Yes, several times

Q18 Please specify

The dissemination of illegal content seems to have been prolific in some areas of content more than others. Reports concerning misinformation and disinformation content, particularly on social media are rife.

Due to COVID-19 pandemic responses around the world, many States adopted a range of restrictions, limiting the movement of people, closing workplaces and schools. Many people were home more often. As a result, both adults and children have increased time spent online. This led to a higher dissemination of content on the Internet, including illegal content due to a combination of increased opportunity and factors of stress, social isolation, and boredom of being home. In particular, many experts expressed concerns that this resulted to a rise in the production, distribution and use of online child exploitation, often for profit (ECPAT, 2020; EUROPOL, 2020; UNICEF, 2020). Reports were also coming from the police in some countries about increases in online offending (National Crime Agency, 2020).

[1] Henitsoa Rafalia, 'Illegal trade in fake or faulty COVID-19 products booming, new UN research reveals' *UN News* (8 July 2020) <https://news.un.org/en/story/2020/07/1067831> accessed 5 August 2020.

The sharp rise in global remote working raised the opportunities for intellectual property law breaches. The dissemination of illegal content was also supported by weaker businesses' network security in a time of general remote working and, more generally, by the suspension or reduced activity of government agencies regularly engaged in detecting such content. For instance, terrorist groups may see opportunities for terrorist activities and terrorist related content online while government attention is focused on the fight against COVID-19.

Q19 N/A

Q20 What actions do online platforms take to minimise risks for consumers to be exposed to scams and other unfair practices (e.g. misleading advertising, exhortation to purchase made to children)?

Online platforms struggle to deal with the volume of content which is illegal and which is regarded as a priority to tackle – such as terrorist content or child sexual abuse material. It is unclear what practices as a whole the sector implements in dealing with the minimisation of risks to consumers of scam exposure and unfair practices.

Comment [KB1]: Note for Edina / full response team

Perhaps from the wider team someone can add comment about targeted ads?

The UK registered Advertising Standards Authority (ASA) launched a UK Scam Ad Alert system in partnership with the major digital advertising and social media platforms, including Facebook and Google, to help tackle fraudulent ads. Consumers can now report scam ads appearing in paid-for space online. ASA then sends an alert to partners, namely all participating platforms with key details of the scam ad, as well as to publishers when the ad appeared on a publisher owned site. If the partners locate them, they will remove the offending ad and suspend the advertiser's account. In some instances, they may also add them to blocklists, even when the ads were not appearing on their platform, stopping them from appearing in future. Consumers can also report all types of scams to Action Fraud, the UK's national reporting centre for fraud and, for international scams, to Econsumer.gov.

Some marketplaces are actively monitoring their online platforms for scams, excessive pricing and misleading health claims, removing listings and/or suspending accounts of third-party sellers, and are also calling for increased support from authorities to identify rogue traders. In the European Union, for example, some have established channels to flag illegal content to member states' authorities.

Online platforms are also informed of scams and other unfair practices by governmental authorities. On 20 March 2020, the consumer protection authorities of the EU member states (Consumer Protection Cooperation network) issued a common position on the most reported scams and unfair business practices on online platforms in the context of the coronavirus outbreak in the EU, which the European Commission subsequently discussed with key online platforms.[2]

[2] European Commission Consumer Cooperation Protection Network, 'Common Position of the Consumer Protection Cooperation Authorities' (20 March 2020) <https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/documents/cpc_common_position_covid19.pdf> accessed 5 August 2020

Q21 Do you consider these measures appropriate?
No.

Q22 Please explain.

The COVID-19 crisis has underscored the interconnected nature of the global community, and the need to support cross-border e-commerce through enhanced international information sharing and co-operation. Consumer agencies, online platforms, businesses and civil society, should more systematically share best practice, market intelligence and consumer messaging. Some relevant initiatives have already been adopted.

Thus, the US FTC has sent warning letters (some jointly with the US Food and Drug Administration) to more than 60 companies in relation to misleading claims about products including homeopathic drugs, essential oils, traditional Chinese medicine, salt therapy, and vitamin immune boosters. The Consumer Affairs Agency of Japan requested 64 businesses to rectify false or misleading claims related to products such as air cleaners and sanitizers. Canada's Competition Bureau has also issued compliance warnings to businesses to stop false or misleading claims that certain products (facemasks, ventilation, air purification products) can prevent or protect against the virus.

The International Consumer Protection Enforcement Network (ICPEN) has developed social media campaigns to promote consumer reporting of COVID-19 related consumer protection issues, particularly scams. The UN Conference on Trade and Development (UNCTAD) has released information on country initiatives to alert consumers about COVID-19 scams, along with recommendations for governments. Advocacy groups such as Consumers International have contributed guidance on ways to protect consumers from COVID-19 threats.

Governments and other public authorities should:

- Educate consumers about COVID-19 scams, including how to report them.
- Monitor more closely online businesses and issue more systematically compliance warnings to businesses to stop false or misleading claims related to certain products.
- Establish a dialogue with online platforms and businesses about scams and other false practice and, to the extent possible, share information to help identify rogue traders.
- Foster co-operation between agencies with relevant consumer protection mandates, for example via inter-agency taskforces.
- Contribute best practices through OECD and other international fora (e.g. ICPEN and UNCTAD), and notify measures taken against unsafe products, including via the OECD's GlobalRecalls portal.
- Avoid rolling back consumer protection and product safety measures and consider ways to reduce the administrative burdens on business and streamline compliance processes.

Online platforms should:

- Warn consumers about known scams and other false practice and explain more clearly how to report those scams.
- Increase efforts to identify and remove scams or other false practice.
- Communicate regularly with governmental authorities about efforts undertaken and challenges encountered.

Online businesses should:

- Incorporate learnings from behavioural insights in the promotion, sale and delivery of products, and minimise techniques that take advantage of consumers' behavioural biases. Clear messaging to reassure consumers about supply chain robustness may help alleviate panic buying.
- Acknowledge that more consumers may be vulnerable during the crisis and consider needs due to health and safety concerns as well as job and other financial losses.
- Warn consumers about known scams and increase efforts to identify and remove false or misleading advertising.

Part 1B

Q1 N/A

Q3 N/A

Q4 N/A

Q5 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.

Very rarely is there a clear explanation offered as to why content has been recommended – greater transparency is needed here to allow users and consumers to be informed as to their options.

Part 1C

Q1 In your experience, are children adequately protected online from harmful behaviour, such as grooming and bullying, or inappropriate content?

Due to the COVID-19 pandemic responses around the world, many States adopted a range of restrictions, limiting the movement of people and closing schools. Many children were taught online. Technology and virtual platforms became a substitute for the classroom. Children and their families were also turning to digital solutions to support children's socialisation and play (through online games, social media and video chat programs). This expanded use of the Internet may increase children's exposure to online risks. It is even more so that many parents or caregivers may be unfamiliar with new technologies, limiting their ability to engage their children in a discussion about keeping safe online. In addition, parents or caregivers were unable to navigate their children's shift to online learning and recreation while balancing work and other uncertainties related to the pandemic. Furthermore, children themselves are insufficiently educated towards harmful content online. While children aged 13 and older may already be familiar with social media, the pandemic has introduced younger children to social networking tools that may not be designed for them and for which they may have limited preparation. Furthermore, girls, children with disabilities and those perceived to be different or at greater risk of catching or spreading COVID-19 may be at increased risk of online harm, such as online sexual exploitation, bullying and discrimination.

Q2 **To what extent do you agree with the following statements related to online disinformation? (see PDF)**

Fully agree x 3

Fully disagree that internal practices guarantee integrity etc.

Q3 Please explain

Digital platforms are motivated by business interests and enjoy a "non-editorial status" or "host-status" for the content they disseminate. They are not accountable for the content they spread. As a result, platforms have shown that they are vulnerable to manipulation, and to prioritising some interests above others. Beyond this, questions of platform control, governance, accountability have continued to expand with greater levels of concern since the origins of the Internet – the debates are not new, but the issues have grown in significance, and severity. Platforms have grown often without thought to their means of controlling content[3] and without any specific planning of governance mechanisms, nor of systems to address content moderation, which has seen a rapid rise in the number of externally contracted content moderators.[4] Whilst there are some clear commitments from

[3] Stephen Levy, *Facebook – The Inside Story* (Penguin, 2020).

[4] Olivia Solon, 'Facebook is hiring moderators. But is the job too gruesome to handle?' *The Guardian* (4 May 2017) <https://www.theguardian.com/technology/2017/may/04/facebook-content-moderators-ptsd-psychological-dangers> accessed 5 August 2020.

NGOs such as the Web Foundation to enhance e.g. gender equality,[5] these commitments cannot be left to platforms alone – historically platforms have not taken action on these issues to guarantee the factors listed in the table.

Digital platforms are in a position to monitor the information circulated and exchanged through them. They are equally capable of taking action to ensure that certain content is less visible or even eliminated completely. It is up to legislators to impose greater accountability requirements on digital platforms for the content they disseminate within the limits of freedom of expression. Thus, the eCommerce Directive of 8 June 2000 needs amending to change the position of online platforms, and shift their status so that they are no longer mere hosts. [6]

Q4 In your personal experience, how has the spread of harmful (but not illegal) activities online changed since the outbreak of COVID-19? Please explain.

Since the outbreak of COVID-19, disinformation (the deliberate spread of false or misleading information with an intent to deceive) and misinformation (the spread of false information, regardless of whether there is an intent to deceive) have spread worldwide, just like the virus itself. "We're not just fighting an epidemic; we're fighting an infodemic," as Dr Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization, stated at the Munich Security Conference in February 2020.

There is no single source, with different actors driven by largely dissimilar motives producing and propagating false and deceptive information to further their own goals and agendas. For example, some people are using online platforms to spread conspiracy theories, claims that COVID-19 is a foreign bioweapon, a partisan sham, the product of 5G technology, or part of a greater plan to re-engineer the population. Others are spreading rumours of supposedly secret cures such as drinking diluted bleach, eating bananas or turning off one's electronics. Others are using the COVID-19 pandemic for financial benefit, selling test kits, masks and treatments on the basis of false or deceptive claims about their preventive or healing powers.

Q5 What good practices can you point to in tackling such harmful activities since the outbreak of COVID-19?

Some platforms have taken important steps, such as directing users to official sources when searching for COVID-19 information, banning ads for medical masks and respirators, and reinforcing their efforts to detect and remove false, misleading and potentially harmful content related to COVID-19, including by terminating online shops or removing listings that make false or deceptive claims about products preventing or curing COVID-19.

Thus, Facebook and Instagram banned ads suggesting that a product is a guaranteed cure or that it prevents people from contracting COVID-19 as well as ads and commerce listings for

[5] Tim Berners-Lee, 'Why the web needs to work for women and girls' *Web Foundation* (12 March 2020) <https://webfoundation.org/2020/03/web-birthday-31/> accessed 5 August 2020.
[6] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

masks, hand sanitisers, surface disinfecting wipes and COVID-19 testing kits. Twitter implemented comparable measures under its Inappropriate Content policy. Similarly, Google and YouTube prohibited any content, including ads, that sought to capitalise on the pandemic, and on this basis they have banned ads for personal protective equipment.[7]

Moreover, Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter and YouTube have published a joint statement on their collaboration with government healthcare agencies to combat fraud and disinformation about COVID-19.[8] In general, there are three main types of collaborative efforts between platforms and public health authorities:

- Highlighting, surfacing and prioritising content from authoritative sources. Platforms like Facebook, Instagram, TikTok and Pinterest are redirecting users to information from the WHO in response to searches for information on and hashtags associated with COVID-19. Similarly, Google launched a one-stop-shop COVID-19 microsite and an "SOS Alert", which directs people searching for "coronavirus" to news and other content from the WHO. YouTube features videos from public health agencies on its homepage and highlights content from authoritative sources in response to searches for information on COVID-19. Twitter, in turn, features a COVID-19 event page with the latest information from trusted sources on top of users' timelines. Snapchat has also partnered with the WHO to create filters and stickers that provide guidance on how to prevent the spread of the virus.
- Co-operation with fact-checkers and health authorities to flag and remove disinformation. Facebook co-operates with third-party fact checkers to debunk false rumours about COVID-19, label that content as false and notify people trying to share such content that it has been verified as false. Facebook partnered with the International Fact-Checking Network (IFCN) to launch a USD 1 million grant programme to increase their capacity and has been removing content flagged by public health authorities, including "claims related to false cures or prevention methods — like drinking bleach cures the coronavirus — or claims that create confusion about health resources that are available". Likewise, reports note Google donated USD 6.5 million to fact-checkers focusing on coronavirus. In turn, Twitter broadened the definition of harm on its platform to address content that goes directly against guidance from authoritative sources of global and local public health information.

[7] OECD, 'Combatting COVID-19 disinformation on online platforms' (3 July 2020) <https://www.oecd.org/coronavirus/policy-responses/combatting-covid-19-disinformation-on-online-platforms-d854ec48> accessed 5 August 2020.

[8] Catherine Shu & Jonathan Shieber, 'Facebook, Reddit, Google, Linkedln, Microsoft, Twitter and YouTube issue joint statement on misinformation' *TechCrunch* (17 March 2020) <https://techcrunch.com/2020/03/16/facebook-reddit-google-linkedin-microsoft-twitter-and-youtube-issue-joint-statement-on-misinformation/> accessed 5 August 2020.

- Offering free advertising to authorities. Facebook, Twitter and Google have granted free advertising credits to the WHO and national health authorities to help them disseminate critical information regarding COVID-19.

Part 1D (this is for organisations but I think organisations dealing with content, not BILETA)

Q1 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?

Yes. Some platform reports, and some reports from specialist agencies with specific remits e.g. Fundamental Rights Agency reports on hate speech reporting and actions by platforms.

Q3 N/A
Q4 N/A
Q5 N/A
Q6 N/A
Q8 N/A
Q10 N/A
Q11 N/A
Q13 N/A
Q14 N/A

Responsibility	Response

PP20-27

Q1 See table below

Maintain an effective 'notice and action' system for reporting illegal goods or content	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)
Maintain a system for assessing the risk of exposure to illegal goods or content	Yes, only platforms at particular risk of exposure to illegal activities by their users
Have content moderation teams, appropriately trained and resourced	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)
Systematically respond to requests from law enforcement authorities	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)
Cooperate with national authorities and law enforcement, in accordance with clear procedures	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)
Cooperate with trusted organisations with proven expertise that can report illegal activities for fast analysis ('trusted flaggers')	Such measures should not be required by law
Detect illegal content, goods or services	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)
In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)
Request professional users to identify themselves clearly ('know your customer' policy)	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)
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)	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)
Inform consumers when they become aware of product recalls or sales of illegal goods	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)
Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities	Such measures should not be required by law
Be transparent about their content policies, measures and their effects	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)
Maintain an effective 'counter-notice' system for users whose goods or content is removed to dispute erroneous decisions	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)

Q2 N/A

Q3 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;
Reason why the activity is considered illegal;
Description of the activity.

Q4 Please explain

When notifying a platform, it is insufficient to merely notify without offering some contextual awareness and explanation for the notification including why there has been such a notification. In order to allow a platform to be notified of potential illegal activity, it is necessary for the platform to be given information on which to make an assessment and then respond – not providing information requires the platform to take steps to make decisions without the context, but also inevitably delays the time for a decision. Speed and ease should be considerations in assessing notifications of illegality – given the volume of reporting, this should be as straightforward and as comprehensive as possible for users and third parties.

Q5 How should the reappearance of illegal content, goods or services be addressed, in your view? What approaches are effective and proportionate?

Reappearance should be addressed through reporting mechanisms but with an enhanced set of responses. In any event, illegal content should be taken down, with an explanation sent to the user who notified, and also to the originator of the content. Further infractions of repeated content or reappearances should trigger an escalated response from the platform, including temporary suspension of service access for example, on a graduated scale.

Q6 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?

Automated tools are a potential element but not the entire solution. As has been widely reported, the use of automated content filters and automated moderation is a significant risk to free expression. Without proper transparency, accountability and due process, automated content moderation is more likely to have a chilling effect on free speech. Furthermore, the resort to automatic tools may lead to the removal of legal content erroneously. For instance, there have been multiple reported incidents of automated monitoring systems flagging COVID-19 content from reputable sources as

spam.[9] Automated tools lack the ability to make decisions in the context of other factors beyond the sole post or content in question [ref needed]. As such, relying purely on automated tools without human oversight is particularly problematic for protecting fundamental rights whilst balancing safety and legality of content. The use of automated tools presents real and significant risks, not only for fundamental rights, but also worsening transparency and accountability[10] alongside risks of over-removals and unjustified takedowns which in turn need human review. Automated moderation systems also risk harm being caused to human oversight reviewers given the volume of problematic and / or illegal content that they need to evaluate.

Q7 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?

The spread of illegal content across multiple platforms and services must be addressed in a consistent manner. Where legal rules are implemented, they must be capable of application across all services so as to ensure that the same illegal content is addressed irrespective of the platform it is hosted on. To have customised sets of legal regulations would create a system that is too burdensome, yet each platform ecosystem and governance mechanisms must be proactive in policing their service within the parameters of the legal framework. This presents particular challenges for services established outside of the European Union yet where platforms operate – for end users – within the European Union system, they must be required to be compliant with the European legal framework.

Q8 N/A

Q9 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?

Responsibilities of other entities should be to feed in to discussions concerning a holistic framework with 'joined up thinking' especially concerning gender equality online.[11] Frequently regulatory discussions at European levels have focussed on specific issues such as e.g. terror-related content[12] or racism, xenophobia and intolerance,[13] or have adopted

[9] Chris Stokel-Walker, 'As humans go home, Facebook and YouTube face a coronavirus crisis' *Wired* (20 March 2020) <https://www.wired.co.uk/article/coronavirus-facts-moderators-facebook-youtube/> accessed 5 August 2020.
[10] Hannah Bloch-Wehba, Automation in Moderation, *Cornell International Law Journal* (forthcoming, 2020) <https://ssrn.com/abstract=3521619> accessed 3 August 2020.
[11] Kim Barker & Olga Jurasz, 'Online violence against women as an obstacle to gender equality: a critical view from Europe' *European Equality Law Review* 2020(1) 47-60 https://www.equalitylaw.eu/downloads/5182-european-equality-law-review-1-2020-pdf-1-057-kb, 58.
[12] European Commission, Recommendation C (2018) 1177 (final) of 1 March 2018 on measures to effectively tackle illegal content online.

broad-brush regimes with unintended consequences as technology has developed, such as the liability shield within the eCommerce Directive.[14] Where civil society, equality bodies, and other NGOs have interests in contributing to discussions of illegal activities – such as those inciting online violence against women for example – they should be invited to take responsibilities in actively contributing to discussions concerning illegal content and activities. It is difficult to perceive a way in which these bodies could be construed as having a *right* to contribute, and there should be no requirement that they do so given their number, and respective breadth of interests.

Q10 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?

Harmful but not illegal content poses unique problems in that there is no legal threshold to act upon it. As such, appropriate and proportionate measures here would rest with the platforms under guidance (but not per se legal rules nor obligations) to act. Harmful content is problematic legally because of the context surrounding it which may or may not make it legal or illegal. As such, trying to establish legal rules concerning harmful but legal content should be avoided – a balance must be struck between fundamental rights and legal protections, and whilst there is a significant volume of content which may be harmful, this is no reason to prevent its dissemination. Similarly, attempting to make harmful content which does not reach established legal thresholds to comprise a criminal offence, illegal poses additional encroachments on freedom of expression rights. User based controls about content that can be muted or filtered out of individual feeds is an appropriate route for addressing content which may cause harm, but which is not illegal.[15] it should also be remembered when dealing with content online that removal is not the only response to consider – other mechanisms include, for example, counter-speech.[16]

People need the skills to navigate and make sense of what they see online safely and competently, and to understand why it is shown to them. This includes knowing how to verify the accuracy and reliability of the content they access and how to distinguish actual news from opinions or rumours. To this end, collaboration between platforms, media organisations, governments and educators is critical. For instance, the partnership between the European Union, UNESCO and Twitter to promote media and information literacy amid

[13] Council Framework Decision 2008/913/JHA of 28 November 2008 on combatting certain forms and expressions of racism and xenophobia by means of criminal law: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008F0913>.

[14] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[15] Kim Barker & Olga Jurasz, 'Online violence against women as an obstacle to gender equality: a critical view from Europe' *European Equality Law Review* 2020(1) 47-60 https://www.equalitylaw.eu/downloads/5182-european-equality-law-review-1-2020-pdf-1-057-kb, 48.

[16] Molly K Land & Rebecca J Hamilton, 'Beyond Takedown: Expanding the Toolkit for Responding to Online Hate' in Predrag Dojcinovic (ed) *Propaganda, War Crimes Trials and International Law: From Cognition to Criminality* (Routledge, 2020), 143.

the COVID-19 disinformation crisis is a laudable initiative that should be replicated by other platforms and relevant stakeholders.[17]

Q11 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.

Given that the pandemic is bringing younger children into education and social networks (some for the first time), online platforms should make significant efforts to help them, and their parents and caregivers, learn to use online resources safely. This includes: Adapting online safety resources to different age groups and making these resources more accessible on their platforms to inform children, parents and caregivers of online risks and provide access to support services. Offering clearly signposted and easy to use technical tools and solutions (e.g. 'parental controls') which can empower parents and caregivers to help their children experience digital technology in an age-appropriate way. Amplifying messaging on safe and responsible behaviour online and supporting children to develop 'digital resilience' skills – in other words, knowledge of how to navigate and respond to risks.

Companies that are developing and deploying virtual classrooms and other education-specific platforms should make sure that safety features are integrated and enhanced and clearly accessible to educators, parents and students. Social networking platforms used for teacher-student interactions should employ built-in protection measures for children while giving adult teachers appropriate permissions to carry out their functions. Furthermore, online platforms using video conferencing services, which are increasingly being used for online interactive sessions, should ensure that relevant security and privacy protections are in place.

Online platforms should promote and facilitate child safety referral services and helplines for children and youth out of school, some of whom may be at increased risk of psychosocial stress, violence and exploitation. This includes sharing information on referral and other support services available for youth, such as national Child Helplines. Companies can seek to increase child helpline capacity with cloud-based infrastructure and by leveraging Interactive Voice Response (IVR)/bot systems to automate helpline queries.

17 UNESCO, 'European social media campaign to address disinformation on Covid-19 & #ThinkBeforeSharing', 21 April 2020 <https://en.unesco.org/news/european-social-media-campaign-address-disinformation-covid-19-thinkbeforesharing> accessed 5 August 2020.

Q12 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.

Measure	Response
Transparently inform consumers about political advertising and sponsored content, in particular during election periods	5
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with user complaints	4
Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives	5
Transparency tools and secure access to 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	4
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	4
Adapted risk assessments and mitigation strategies undertaken by online platforms	4
Ensure effective access and visibility of a variety of authentic and professional journalistic sources	3
Auditing systems for platform actions and risk assessments	4
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.	5
Other (please specify)	4

Q13 Please specify

Education in new information and communication technologies appears essential for the development for the prevention of harmful effects of false information, in particular in electoral campaigns. Only citizens trained in the analysis of digital information can have enough distance and a critical mind to apprehend that information. The lasting solution to the fight against misinformation is educating citizens for responsible use of mass media and social media. Learning the codes and languages of digital media is the best method to be able to differentiate quality information from false information. Such is also the conclusion of the group of experts set up by the European Commission to advise on policy initiatives to tackle fake news and disinformation spread online.[18] It proposes strengthening media and information literacy to counter disinformation and help users navigate the digital media environment. Online platforms could contribute to the improvement of media and information literacy.

Q14 N/A

[18] Report of the independent high-level group on fake news and online disinformation. March 2018 <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation)> accessed 5 August 2020, 25-27.

Q15 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).

Measure	Response
High standards of transparency on their terms of service and removal decisions	5
Diligence in assessing the content notified to them for removal or blocking	5
Maintaining an effective complaint and redress mechanism	4
Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended	5
High accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts	5
Enabling third party insight – e.g. by academics – of main content moderation systems	5

Q16 Please explain

Oversight and accountability must play a role in the regulatory paradigms being considered. Legal provisions need enforcement measures in order to be effective, and even then, this is not always the situation. Allowing third party insight – or for example, auditing by external bodies or academics[19] – of the main content moderation systems would enhance the accountability of such approaches. Similarly, by allowing – and actively requiring – an independent oversight mechanism, transparency, reporting and critique would be allowed, potentially paving the way for best practice models to emerge whilst protecting rights and ensuring compliance with legal obligations to address illegal content.

Q17 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?

Other concerns do exist (see above at answers to Qs 9&10) but given the seeming low priority these other concerns receive from platforms and services online, there are few effective mechanisms that feed into the regulatory paradigm. Mechanisms should be tailored to these concerns. Legal obligations for e.g. gender equality should be considered but enforcement will remain problematic in the absence of legal requirements to tackle such issues proactively in non-state actors.

In attempting to address other concerns, best practice should be explored with NGOs and civil society. Whilst attempting to address 'everything' online, inevitably divergent approaches will emerge which are favoured for distinct issues – there will be some nuance but attempting to capture everything could lead to situations where the regulations are ineffective and too broad. Equally, attempting to have specific mechanisms for each area of potential illegality online is likely to result in a situation which is too cumbersome.

[19] Max Beverton-Palmer and Rosie Beacon, 'Online Harms: Bring in the Auditors' Institute for Global Change (30 July 2020) <https://institute.global/policy/online-harms-bring-auditors> accessed 05 August 2020.

Q18 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.

Online platforms should be very clear what their policies are for dealing with illegal content, and illegal goods. The information should be easily accessible from their 'rules' pages, and should be presented in easy to read formats, as well as formats for the visually impaired. The easy to read format should spell out simply what is illegal content or goods, how to report it on that platform, and what will happen next. The full policy should offer an example flow chart of how the process is then undertaken internally with likely timescales and should offer an overview of how to appeal a decision.

The information which platforms should make available in respect of measures taken should at a minimum list the following:

- Category of content or goods
- Reason for report
- Date of report
- Outcome of report
- Reason (in brief) for outcome
- Method of challenging outcome decision

The last three categories of information in this list should be provided to the person(s) making the report once an outcome has been reached, as well as the original poster / account that provided the content. The individual information should be amalgamated and produced into monthly reports of statistics, and quarterly reports with full information. These reports should be freely available on the relevant platform website but should also be provided to the relevant oversight body.

Q19 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?

The information to be shared with trusted researchers and other third parties in respect of automated systems for detection, removal and blocking should include all of the information listed in Q18 above, along with details of the number of instances where automated systems made a decision, the number of instances where that decision was reviewed and altered by a human moderator, the number of instances where an automated decision was challenged by a user of the service, and the outcome of those challenges. In addition, trusted researchers should be allowed access to governance meetings where discussions concerning the effectiveness or otherwise of the automated system are held. The role of trusted third parties here would be in effect 'observer' status, to report back to

oversight bodies on the effectiveness of addressing illegal content or goods by each platform.

Q20 N/A

Q21 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 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

Q22 Please explain. What would be the benefits? What would be concerns for companies, consumers or other third parties?

Potential benefits include the ability to respond in a timely manner to requests of law enforcement bodies. Other benefits include the ability to share practice, and to highlight prolific content or accounts across platforms that persistently post or share illegal content or propose illegal goods – such shared knowledge and clustering may allow for an escalated set of responses beyond individual platforms, and allow law enforcement bodies to have a critical mass of evidence across a number of platforms in order to take legal action against those posting the content rather than relying upon the platforms to repeatedly detect and remove. Inevitably concerns will arise about sharing knowledge and information, and how that information has been gathered but there should be no need to share proprietary information across platforms. Privacy concerns may be voiced by consumers or users but if such steps are capable of being taken within the limitations of the GDPR, a balance continues to be struck.

Q23 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)?

Comment [KB2]: Note for Edina / full response team

This may need tweaking in light of the final module answers provided by other members of the response team]

Fines dependent on profit share and market dominance are likely sanctions which could be proportionate. The problem with such a step is that the size of the revenue that online platforms generate makes it difficult for even sizable fines to be much of a deterrent. Fiscal taxes or licensing may be a viable option.

Q24 Are there other points you would like to raise?

Online platforms are non-state actors – but are commercial entities with business operations in multiple countries and legal jurisdictions. As such, EU mechanisms – legislated upon or not – are still subject to interpretation by Member States across these various legal borders. Consequently, where there are vagaries in definitions of behaviours and / or obligations imposed on platforms, legislative precision is essential in order to limit the potential for platforms avoiding (or limiting) their obligations.

Education in media and information literacy should be developed. Only users trained in the analysis of digital information can have enough distance and a critical mind to apprehend that information (see above at answer to Q 13)

PP52-53

Not in BILETA remit – suggest leave unanswered.

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.
2The 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

0 / 5000

Section 4 of the E-Commerce Directive includes some provisions governing the liability of online intermediaries. In that section, Articles 12, 13 and 14 of the E-Commerce Directive 2000/31 each contain, within paragraph 1 respectively, an exemption for 'mere conduit', 'caching' and 'hosting' activities also known as the safe harbour framework. Articles 12 to 15 of the E-Commerce Directive stem from the US Digital Millennium Copyright Act 1998, which envisaged similar exemptions from liability, but in the copyright context. These are included in Title 17, Chapter 5, Section 512 of the US DMCA.

Mere conduit, caching, hosting are not mutually exclusive classifications; thus, it is possible for an online intermediary to provide services, which fall into more than one classification. For example, the US Copyright Office has noted that Alphabet provides Google search services (along with online cashing of some indexed sites) and YouTube and Blogger hosting sites, together with different sites such as, advertising services, which do not easily fall into any of the section 512 classifications. This is in the same way as Articles 12, 13 and 14 of Directive 2000/31. Equally, other current site models blur the lines between mere conduit and hosting sites https://www.copyright.gov/policy/section512/section-512-full-report.pdf see page 23.

Firstly, as Section 512(h) of the US DMCA, the language of Article 12 of the E-Commerce Directive is unclear since it also raises issues as to whether it is applicable to mere conduit online intermediaries, who for instance could be the only source of data concerning the identity of users taking part in often unlawful activities such as, peer-to-peer filesharing. Therefore, it would be advisable for EC to provide some clarification regarding the language of Article 12 of the E-Commerce Directive https://www.copyright.gov/policy/section512/section-512-full-report.pdf see page 6.

On the other hand, Article 13 of the E-Commerce Directive does not seem to be as much of a problem as the other two safe harbors that is, 'mere conduit' and 'hosting'. As in the US, the caching safe harbor has not attracted much judicial attention in the EU https://www.copyright.gov/policy/section512/section-512-full-report.pdf see page 92.

In terms of the 'hosting' exemption, in 2000, the E-Commerce Directive followed the example of a neutral hosting service, whose activity 'is of a mere technical, automatic and passive nature' as per recital 42 of the E-Commerce Directive. Originally, the CJEU in joined cases C-236/08 C-237/08 and C-238/08 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (C-236/08), *Google France SARL v Viaticum SA and Luteciel SARL* (C-237/08) and *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL* [2010] and C-324/09 *L'Oréal SA and others v eBay International AG and others* [2011] ECR I-0000, the CJEU considered Article 14 to apply exclusively to offering services neutrally by a simply technical and automatic processing of information provided to its users. However, not all hosting services have played a passive role. For example, Nordemann has noted that some hosting services have played an active role regarding the data stored specifically by branding, indexing and suggesting:

'*Example 1: eBay is in general categorised as a hosting provider. But eBay has been found to provide assistance which entailed, in particular, optimising the presentation of the offers for sale in question or promoting those offers, for example through advertising third party eBay offers with own advertisements on the Google search engine. The CJEU found that eBay in such cases played an "active role" and would no longer come under the liability privilege of the hosting provider in Article 14 E-Commerce-Directive.The CJEU made clear, however, that it is not sufficient to exclude the application of Article 14 E-Commerce-Directive if the service provider is remunerated for the service and provides general information to its customers. Example 2: In a German case, the Hamburg Court of Appeal confirmed that YouTube would no longer come under Article 14 E-Commerce Directive, as YouTube would give individualised music recommendations to interested users and would suggest next to the viewed videos further (presumably) interesting videos. Furthermore, YouTube would play an active role excluding Article 14 E-Commerce Directive when providing extensive user friendly functions for the use of the music provided on YouTube such as search, categories with genres, filtering, marking, playlists, playing functions, recommendations to third parties etc*.' https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614207/IPOL_IDA(2017)614207_EN.pdf see pages 9 and 10.

Another issue for the EC to address is the persistent reliance upon Articles 12 to 15 of the E-Commerce Directive's function-based safe harbors, particularly today that most online intermediaries provide multiple services and thus could fall under numerous safe harbors.

For instance, should bookmarking services, which display a text snippet or image from the service be regarded as an information location tool - which unlike the US DMCA 1998 this is not regulated under the E-Commerce Directive - or a content host under Article 14? Is it relevant whether the service automatically chooses the text snippet or image, or if it is selected by the customer? Equally, should content delivery services be considered caching sites under Article 13, or instead mere conduits under Article 12? Is it relevant to the answer who the user for these sites is ie the distributer/ content owner themselves or a third party online intermediary? https://www.copyright.gov/policy/section512/section-512-full-report.pdf see page 95

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).

3Are there aspects that require further legal clarification?

5000 character(s) maximum

0 / 5000

In joined cases C-682/18 and C-683/18 *Frank Peterson v YouTube* [2020] ECLI:EU:2020:586 [169], the AG stated that, pursuant to Article 14(1) of the E-Commerce Directive, an online intermediary could not be held liable for the data that it stored at users' request as long as (a) it did not have 'actual knowledge of illegal activity or information' and, concerning claims for damages, it was not 'aware of facts or circumstances from which the illegal activity or information is apparent' or (b) on acquiring this knowledge, it acted 'expeditiously to remove or to disable access to the information'. However, as the AG noted, one question that required further legal clarification was whether the requirement laid down in Article 14(1)(a) of the E-Commerce Directive referred to specific unlawful data – see [AG 170]. Importantly, the AG stressed that the answer to this issue had significant ramifications wherever online intermediary liability was sought for unlawful data that it stored. In sum, the issue was whether, so as to refuse the online intermediary affected the exemption encapsulated in Article 14(1) of the E-Commerce Directive, the claimant had to demonstrate that the online intermediary possessed 'knowledge' or 'awareness' of the data specifically or whether it possessed abstract and general 'knowledge' or 'awareness' of the fact that it stored unlawful data and that its services were utilised for unlawful activities – see [AG 171].

Moreover, in joined cases C-682/18 and C-683/18 *Frank Peterson v YouTube* [2020] ECLI:EU:2020:586, the AG also explained that the E-Commerce Directive did not provide any safeguards for users, for instance, a 'counter-notification' process for contesting the 'over-removal' of their data. According to the AG, Recital 46 of Directive 2000/31 simply asserted that Member States might set out 'specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information' – see paragraph [AG 189]. In this context, it would be advisable for the EC to provide some clarity on what these 'specific requirements' may entail.

Moreover, in joined cases C-682/18 and C-683/18 *Frank Peterson v YouTube* [2020] ECLI:EU:2020:586, the AG also noted that the question whether the 'facts or circumstances' brought to the attention of an online intermediary were enough to give it 'awareness' of unlawful data under Article 14(1)(a) of the E-Commerce Directive was determined by the varying circumstances of each case, specifically: (i) the extent of accuracy of the notification; (ii) the complexity of the analysis needed to appreciate the unlawfulness of the data; (iii) and the resources accessible to the online intermediary. The AG stressed that the same applied to the question whether the online intermediary acted 'expeditiously' within the meaning of Article 14(1)(b) of the E-Commerce Directive – see paragraph [AG 190]. Therefore, all these elements would additionally require further legal clarification.

It is worth noting that the above problem has also been highlighted by the US Copyright Office, which has stressed that another major inefficiency in the US Digital Millennium Copyright Act 1998 DMCA is the lack of clarity on what is understood by 'expeditious' takedown. The US Copyright Office points out that the DMCA does not provide any clear guidelines on what means the word expeditious. According to the US Copyright Office, the statutory condition that online intermediaries 'expeditiously' delete or disable access to unlawful content on becoming aware of it, it is to be interpreted by the courts relying on a flexible view, which takes into account all the circumstances of each case. The US Copyright Office broadly agrees that such flexibility is required. On the other hand, it also notes that the actual statutory timeframes to continue granting access to material after receipt of a counter-notification ill serves both content owners and users in view of current business models, as well as the existence of litigation. The US Copyright Office stresses that 10 to 14 days is both too short for a content owner to reasonably prepare and file lawsuit to preclude the return of unlawful content and too long for lawful expression to be blocked. For this reason, the US Copyright Office recommends that the US Congress might explore an alternative dispute resolution process to address all the above issues instead https://www.copyright.gov/policy/section512/section-512-full-report.pdf see pages 6 and 160.

4Does 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

0 / 5000

The current legal framework under the E-Commerce Directive does not appear to dis-incentivize online intermediaries to take proactive measures against unlawful activities. In joined cases C-682/18 and C-683/18 *Frank Peterson v YouTube* [2020] ECLI:EU:2020:586, the AG explained that, paragraph 3 of Article 14 of the of Directive 2000/31does 'not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement'. The AG noted that such article together with Recital 45 E-Commerce Directive did not preclude an online intermediary being the subject of an injunction – see [AG 198].
Moreover, in joined cases C-682/18 and C-683/18 *Frank Peterson v YouTube* [2020] ECLI:EU:2020:586, the AG also pointed out that it was clear from Case 70-10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 and C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* [2019] EU:C:2019:458, that Article 15(1) of the E-Commerce Directive did not preclude any duty to identify and block. The AG noted that although under Article 15(1) an online intermediary might not be obliged through an injunction to perform general filtering of the data it stored so as to search for any infringement, it did not, a priori, preclude the online intermediary from being obliged to block a specific file that utilises the copyrighted content, which was found to be illegal by a court. The AG elaborated that Article 15(1) did not prevent the online intermediary from being compelled to identify and block not just identical copies of a specific file, but also other equivalent files ie those that utilize the copyrighted content in the same way. Thus, the AG stressed that Article 15(1) of the E-Commerce Directive did not prevent a 'stay down' duty from being imposed upon an online intermediary – see [AG 221].

As the AG noted in footnote 188, a staydown duty was included in Article 17(4) of the EU Directive on Copyright in the Digital Single Market (CDSM). However, the AG also explained that regulators made an exception for 'small' online intermediaries, which did not possess the technology or resources required to adopt such duty. Importantly, the AG concluded that while Article 14(1)(b) of the E-Commerce Directive 2000/31 provided for a takedown duty, on the other hand, Article 17(4)(c) of the CDSM now included an *ex ante* and general staydown duty – see [AG footnote 234].

In this context, it is worth noting that Article 17(6) of the CDSM Directive subjects start-ups and small online intermediaries which have existed for less than 3 years with a turnover below 10 million euros to simpler obligations. According to Article 17(6), if these small online intermediaries fail to conclude an agreement with rightholders, following a rightholder notice, they must respond expeditiously to remove or disable access to the unlawful content by implementing notice and takedown. Notwithstanding, if at a later stage the audience surpasses 5 million visitors monthly, upon receiving a rightholder notice, such small online intermediaries must also make best efforts to prevent future uploads by adopting notice and staydown.

Arguably, in view of the AG's finding in joined cases C-682/18 and C-683/18 *Frank Peterson v YouTube* [2020] ECLI:EU:2020:586 above, the CDSM Directive fails to recognise, that to enable matching of content the creation of centralised databases of copyrighted material is critical to successful upload filter performance - Gann, A., and D. Abecassis. 2018. "The Impact of a Content Filtering Mandate on Online Service Providers." https://www.analysysmason.com/Consulting/content/reports/the-impact-of-a-

content-filtering-June2018/ see page 4. In C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [46], [47] and C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [48], [49], the CJEU held that as staydown injunctions compelled services to deploy costly, complex, permanent upload filters at their own expense, this violated the freedom to conduct their business under Article 16 of the EU Charter. Therefore, one might argue that unless databases were centralised and exclusively targeted music and video with high-commercial value content, the implementation costs of Article 17 could dramatically increase. This is because it would be essential to compare every fingerprint against numerous databases for numerous rightholders and numerous types of material. Within industries where fragmentation is reduced, such as in the music industry, rightholders are generally able to combine efforts to create centralised databases. However, for most other types of content, such as images, databases tend to be rightholder-specific and fragmented. Moreover, since the OCSSP would need to deploy multiple upload filters to individually detect every work, the use of each supplementary database would thus duplicate Article 17 implementation expenses (Gann and Abecassis 2018, 7, 9, 11, 12). Indeed, this notably conflicts with C-27/76 *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* [1978] ECR 207 [24] and C-322/81 *NV Nederlandsche Banden Industrie Michelin v Commission of the European* Communities [1983] ECR 3461 [29] where the CJEU found that Article 86 of the Treaty on the Functioning of the EU (TFEU) reflected the main goal of Article 3(f) TFEU, namely, adopting a framework which ensured that common market competition was never distorted - see also C-52/09 *Konkurrensverket v TeliaSonera Sverige AB* [2011] [2011] ECR I-527 [20]-[22].Thus, it seems inevitable that Article 17 of the CDSM would harm competition and stifle innovation.

5Do 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.

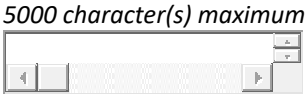
As the CJEU case-law suggests, there are good reasons to believe that, pursuant to Recital 42 of the E-Commerce Directive, the concept characterising online intermediaries as playing a role of a 'mere technical, automatic and passive nature' in the transmission of information is sufficiently clear and still valid today.
In joined cases C-236/08 C-237/08 and C-238/08 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (C-236/08), *Google France SARL v Viaticum SA and Luteciel SARL* (C-237/08) and *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL* [2010], the CJEU found that an online intermediary might benefit from the liability exemption under Article 14 of the E-Commerce Directive for data that it stores at users' request just provided that its conduct is restricted to that of an online intermediary in the context of Section 4 of Directive 2000/31. The CJEU noted that under Recital 42 E-Commerce Directive it was necessary to asses 'whether the role played by that service

provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores' or whether, by contrast, it plays 'an *active role* of such a kind as to give it knowledge of, or control over, the data stored' – see [137].
Equally, in C-324/09 *L'Oréal SA and others v eBay International AG and others* [2011] ECR I-0000, the CJEU found that an online marketplace operator might benefit from Article 14(1) of the E-Commerce Directive as long as the service provided involved the storage of data supplied by the users of the marketplace. The CJEU also noted that an online intermediary might benefit from the liability exemption as per Article 14(1) just if it was an online intermediary. It explained that this was not the case where that online intermediary, 'instead of confining itself to providing that service neutrally by a merely technical and automatic processing of the data provided by its customers, plays an active role of such a kind as to give it knowledge of, or control over, those data' - see [110 to 113].
Taken together, as the AG noted in joined cases C-682/18 and C-683/18 *Frank Peterson v YouTube* [2020] ECLI:EU:2020:586, it was clear from the above rulings that online intermediaries that engage, as part of their activity, in the storage of data supplied by their users, might benefit from the liability exemption included in Article 14(1) of the E-Commerce Directive, provided that they had not played an 'active role' of such a type as to provide them with knowledge of, or control over the data at issue – see [AG 150].

The AG explained that an online intermediary storing data supplied by its users necessarily had some control over that data. Specifically, it had the technical capability to delete or to disable access to that data. The AG noted that, under Article 14(1)(a) and (b) of Directive 2000/31, the online intermediary was expected to act in this way concerning unlawful data of which it was made aware. This control capability cannot, per se, indicate that an online intermediary played an 'active role', otherwise Article 14(1) of the E-Commerce Directive would be void of any effectiveness - see [AG 151].Indeed, the AG stressed that the 'active role' understood by the CJEU correctly related to the actual content of the data supplied by users. According to the AG, the CJEU's case-law means that an online intermediary played an 'active role' of such a type as to provide it with 'knowledge of, or control over', the information that it stored at users' request if it did not merely engage in the processing of that data that was neutral vis-à-vis its content, but if, by the nature of the activity, it was considered to obtain intellectual control of that information. The AG indicated that this was particularly the case if the online intermediary selected the stored data, it was actively engaged in the content of that data in some other way or if it presented that data to the users in such a manner that it seemed to be its own. The AG highlighted that in those circumstances, the online intermediary went beyond the role of an intermediary for data supplied by its users; in other words, it appropriated that data - see [AG 152].
Moreover, in joined cases C-682/18 and C-683/18 *Frank Peterson v YouTube* [2020] ECLI:EU:2020:586 the AG also noted that the fact that the data stored could be downloaded or viewed on platforms such as, YouTube did not suggest an 'active role' on the part of their operators. According to the AG, the only important issue was whether the online intermediary controlled the content of the data stored as it was downloaded or viewed at users' request by 'merely technical and automatic' processing - see [AG 155].The AG elaborated that indexing, search and recommendations functions were automated since they entailed 'merely technical and automatic processing' of data stored at users' request,

as acknowledged by the CJEU in C-324/09 *L'Oréal SA and others v eBay International AG and others* [2011] ECR I-0000s. The AG concluded that the fact that the online intermediary devised automated tools such as, algorithms to allow that processing as well as controlling the conditions for showing the search results, did not mean that it had control over the content of the data sought - see [AG 160 to 162].

5000 character(s) maximum



0 / 5000

6The 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.

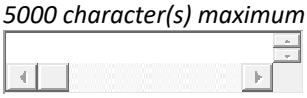
It is submitted that the general monitoring requirement included in the E-Commerce Directive is still appropriate today as it strikes a fair balance between all the competing rights and interests at stake. Indeed, this is expressly acknowledged in the CJEU case-law. In case 360-10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [33]–[34]; see also Case 70-10 *Scarlet Extended SA v Société´ belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [35]–[48], the CJEU observed that Article 15(1) of the E-Commerce Directive prohibited domestic courts from imposing injunctions against social network platforms through general monitoring obligations. The Court remarked that since staydown injunctions obliged these platforms to implement a complex, expensive and permanent system at their own expense, this seriously infringed the freedom to conduct their business. Notably, it held that this technology violated Article 3(1) of Directive 2004/48/EC. Equally, in Case 360-10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [48]–[50]; see also Case 70-10 *Scarlet Extended SA v Société´ belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [51]–[53], the CJEU noted that the filtering measure also entailed the detection, automatic analysis and processing of personal information, probably blocking legitimate communications. It also controversially violated user rights under Articles 8 and 11 Charter. Relying on *Promusicae v Telefonica*, the CJEU found that notice and staydown thus failed to strike a fair balance between, on the one hand, rightholders' right to IP, and on the other social network platforms' freedom to conduct their business, as well as users' right to personal data protection and their right to receive and impart information – see Case 360-10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [51]; see also Case 70-10 *Scarlet Extended SA v Société´ belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [53]; and Case 484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* [2016] [87].

That said, however, the literature seems to identify an existing research gap in that the Court of Justice of the EU (CJEU) has yet to fully clarify the boundary between general and specific monitoring. Article 15 of the E-Commerce Directive prohibits Member State courts

from imposing on service providers a general obligation to monitor stored or transmitted information or actively look for facts or circumstances denoting unlawful action, such as uploading unauthorised copyrighted material. However, importantly, under the E-Commerce Directive, the prohibition of monitoring duties exclusively concerns monitoring of a general character. Recital 47 of the E-Commerce Directive also allows Member States to require services to perform a monitoring obligation in a specifically targeted situation. Moreover, pursuant to Recital 48 of the same Directive, such services can also adopt 'duties of care' to identify and prevent unlawful activities, specified by domestic legislation.

In C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* [2019] EU:C:2019:458, the CJEU explained that, pursuant to Article 15 of the E-Commerce Directive, a duty extending to information with equivalent content did not result in a general monitoring obligation being imposed upon hosting services. The CJEU found that this was particularly the case provided that the monitoring and examination of information required were limited to the information including the details set out in the staydown injunction, and the services were not required to undertake an independent evaluation since they could use 'automated search tools and technologies' – see paragraph [46]. Moreover, the CJEU found that, following a complaint notification, hosting services could be compelled to remove and/or block access to 'identical' and 'equivalent' information previously found to be illegal by Member State courts, even worldwide, provided that the staydown injunction respected international law – see paragraph [53]. In this context, it would be advisable for the EC to clarify what type of information should be set out in the staydown injunction and the parameters for these injunctions to be compatible with international law. For instance, it is arguable that the scope of *ratione personae*, *ratione materiae* and *ratione temporis* of the surveillance and technical measures required to implement monitoring systems should be set out in the injunction that is, the number of users and services to be affected, the types of communications to be impacted and the time to be taken over the measures. Moreover, it should also be clarified the level of examination required to perform user monitoring, namely, Deep Packet Inspection (DPI), Shallow Packet Inspection (SPI) or both.

5000 character(s) maximum



0 / 5000

7 Do you see any other points where an upgrade may be needed for the liability regime of digital services acting as intermediaries?

Lastly, in terms of the liability of internet intermediaries, another issue, which requires further clarification and update is algorithmic transparency. For instance, in Case 70-10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4, the AG observed that notice and staydown entails not only the

filtering of all electronic communications passing via the service provider to identify those implicated in copyright infringement but also the blocking of all incoming and outgoing communications which involved such infringement. However, the AG highlighted that it was impossible to determine the *modus operandi* of these systems, such as the specific criteria under which the monitoring was performed, the filtering methods used and the procedures for detecting infringing material – see [AG 46] [AG 52].

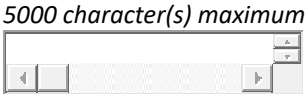
In this context, in agreement with the European Data Protection Supervisor https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf, UN Special Rapporteur David Kaye stressed that, in addition to conducting human rights impact assessments and public consultations on upload filters, developers of monitoring systems should make all filtering criteria fully auditable, allowing regular external and independent auditing and the publishing of results https://www.un.org/ga/search/view_doc.asp?symbol=A/73/348. Importantly, this is consistent with Article 35 of the General Data Protection Regulation which requires services to complete Data Protection Impact Assessments (DPIAs). Indeed, these DPIAs show that appropriate safeguards are in place regarding data processing operations, which are 'likely to result in high risk'.

Moreover, a letter from Dr Clayton, 2 October, 2012, cautions that, before these systems are introduced, the public should also have the right to know how they function that is, the decisions made by algorithms should be transparent and visible. It recommends that to facilitate independent review, some technical details must remain confidential, such as the monitoring system's IP address and commercial keywords, but the rest should indeed be published. Importantly, it concludes that 'secret designs' should not be deemed to produce valid results.

In C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [33]-[38] and C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [33]-[38] the CJEU held that, pursuant to Article 15 E-Commerce Directive, in order to assess whether upload filters led to general monitoring obligations being imposed on services, it was necessary to evaluate whether such services were required to actively monitor 'all the data' of 'all users' to prevent 'any' future copyright violation. Therefore, while this is the most common way to implement upload filters, it remains legally questionable to apply such a method to 'all' files because of the data processor-invasive nature of these filters. This contrasts with C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* [2019] EU:C:2019:458 where the CJEU explained that, pursuant to Article 15 of the E-Commerce Directive, a duty extending to information with equivalent content did not result in a general monitoring obligation being imposed upon hosting services. The CJEU found that this was particularly the case provided that the monitoring and examination of information required were limited to the information including the details set out in the staydown injunction, and the services were not required to undertake an independent evaluation since they could use 'automated search tools and technologies' – see [46].

In this regard, another issue for the EC to consider is how monitoring systems, which rely on upload filters could be implemented in a less data processor-intrusive way for online intermediaries and minimally impact users' rights. For instance, in the context of Article 17 of the EU Directive on Copyright in the Digital Single Market (CDSM) for general monitoring obligations to become lawful 'duties of care' and 'specific' enough to comply with Recitals 47 and 48 E-Commerce Directive, it would be possible to begin with less processor-exhaustive stages to establish whether the transfer includes a registered copyrighted file, and accordingly to move to more processor-exhaustive stages only if previous stages do not return a match – see European Patent Office. 2014. "European Patent Specification." https://www.audiblemagic.com/wp-content/uploads/2014/10/EP1490767B1-1.pdf page 8. Moreover, rightholders could register in a database rules which fully comply with the case-law of the Strasbourg and Luxembourg courts. In particular, there should be the following business rules: first, assessing whether the uploaded material contains a registered work of high commercial value; then, checking the frequency and number of unlawful uploads that is, asking a database for suspected repeat infringement IP addresses; next, sending a message alerting of potential commercial-scale infringement or redirecting to a commercial website; and lastly, giving the opportunity to alleged commercial-scale uploaders to challenge the blocking before actually implementing it – see Romero-Moreno, Felipe (17 March 2020). "'Upload filters' and human rights: implementing Article 17 of the Directive on Copyright in the Digital Single Market". *International Review of Law, Computers & Technology* page 164.

5000 character(s) maximum



0 / 5000

If you're human, leave this field blank 

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

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

The answer is more straight forward than it seems. We agree the factors you have offered are important. Gatekeepers are essentially companies able to control access between businesses and customers; for example, advertisers wishing to reach users of a social media platform, retailers selling to the customers of a popular e-commerce platform, or messaging apps wishing to connect to very large user bases on dominant services. The platforms are able to control access and charge high fees, manipulate rankings or prominence, and control reputations of firms (J Furman, D Coyle, A Fletcher, D McAuley and P Marsden, Unlocking Digital Competition, 2019, 42).

Relatedly, ecosystems are collections of services, connected via privileged channels not fully available to competitors (J Crémer, A de Montjoye and H Schweitzer, Competition policy for the digital era (Luxembourg: Publications Office of the European Union, 2019, 34). For example, the UK Competition and Markets Authority (CMA) visualised the Google and Facebook ecosystems referring to their influence on price, quality and choice in adjacent markets, through the ability to leverage its strong position in its core market into other adjacent markets (CMA, Online platforms and digital advertising, Market study final report, 1 July 2020). Furthermore, In 2018, the European Data Protection Supervisor concluded that AdTech is an ecosystem that "has now been weaponised by actors with political motivations, including those wishing to disrupt the democratic process and undermine social cohesion. Opaque algorithmic decision-making rewards content which provokes outrage, on the basis that greater engagement generates revenue for the platforms in question. This poses obvious risks to fundamental values and democracy."

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

There are many practices of this sort, arising from the platforms' market power, dominance, horizontal and vertical integration, concentration and other effects, explained below. These practices ultimately result in unfair commercial practices directed to consumers and broader more societial harms. These platforms operate on business models based around maximising user attention that has negative side effects, including the amplification of disinformation, hate speech, and extremism. Other concerns include online safety, privacy and data protection, free speech, unfair consumer contracts, harmful advertising, manipulation, and discrimination. More widely, as seen in the Cambridge Analytica scandal, these practices can result in threats to electoral processes, democracy, and the rule of law, Unfairness, therefore, goes beyond data protection, contractual, anti-competitive, or consumer fairness, and affects democratic discourse, the rule of law, as well as autonomy, and the dignity of users and citizens (see e.g. I Graef, D Clifford and P Valcke, Fairness and enforcement: bridging competition, data protection, and consumer law, International Data Privacy Law, 2018, Vol. 8, No. 3).

A concern that various researchers in our community have discussed in detail is content moderation – both of user generated and advertising content. (e.g. Keller, Daphne and Leerssen, Paddy, Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation in N. Persily & J. Tucker, Social Media and Democracy: The State of the Field and Prospects for Reform, Cambridge University Press, 2020; Leiser, Regulating Computational Propaganda, Cambridge International Law Journal, 2019). The issues around automated content moderation, as well as human errors undertaken by platforms often result in practices that restrict free expression/privacy/data protection and thus should be independently verified through both a human rights audit and an impact assessment. The audit should examine compliance top-down and horizontally. Furthermore, unregulated

advertising content can spread hate speech and manipulative disinformation harming democratic discourse without any corrective effects of the marketplace of ideas.

One issue that appears to be receiving increasing attention is the lack of interoperability among platform operators. There is some suggestion that a lack therof reinforces unfair practices by the platforms.. By actively reducing interoperability capabilities, large platforms have been able to adversely affect their competitors, newcomers and consequently, share user behaviour and choice (Ian Brown, Interoperability as a tool for competition regulation, briefing paper, 2020, on file with the authors). For example, Facebook has reduced or blocked access to some of these capabilities since 2010, including stopping Twitter's Facebook app finding other friends using the service, stopping Instagram photos appearing on Twitter, in 2013 cutting off apps "including Vine, Yandex Wonder, Voxer and more" (B Thompson, Portability and Interoperability, Stratechery, 3 December 2019). Also, Facebook's terms and conditions until 2018 included a "non-replication" principle to limit the ability of other tools to provide functionality competing with Facebook's services, as does Twitter's terms and conditions (CMA, 2020, Appendix W, p. 2).

These concerns are further complicated with the lack of data currently available for the evidence-based decision making by regulators. Stark *et al* clarify that content moderation issues (among others) 'should be tackled with reason and based on empirical evidence' and 'scientific evidence is needed on both thematic complexes in order to investigate the extent of the phenomena and their consequences in more detail, so that evidence-based measures can be developed.' (Birgit Stark and others, 'Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse', Algorithm Watch 2020; or Jef Ausloos, Paddy Leerssen, Pim ten Thije, Operationalizing Research Access in Platform Governance: What to learn from other industries?, 25 June 2020). This evidence base can not only assist regulators, but other actors with a stake in effective platform governance such as users, journalists, researchers, and the civil sector. Leiser and Harbinja also argue that there is considerable consequences applying abstract legal obligations like a 'duty of care' to online harm regulation (Leiser and Harbinja, 2021)

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

As stated above, platforms are now in a position to collect vast amounts of data about users and to shape how they interact with each other and their environment. There have been ongoing concerns over the use of personal data, as indicated repeatedly by our wider community and our research (e.g. unclear privacy policies, vague purposes for the processing of personal data, data sharing with advertisers and ad networks, unfair commercial terms related to the collection and sharing of personal data etc; references are too numerous to include here). In this respect, the EU data protection framework could be seen as setting out a *minimum* standard, and recognition that it does not always appropriately address these concerns (e.g. issues around anonymisation practices, PETs and the promises companies have made in this regard recently, fairness is far better aligned with the EU's consumer protection regime). In our view, any steps toward transparency should exceed the GDPR's framework, and include implications processing of anonymised data may have on users, their choice and autonomy. The recnt update of the consumer protection regime should be embraced for ensuring fairness in the way data is used to manipulate choice architecture and to regulate 'dark patterns'.

The rise of surveillance/informational capitalism constantly reinforces data ecosystems, with a notable tendency of concentrating data in the hands of 'central nodes'. These central

nodes, as well as the surrounding ecosystems, are predominantly in private hands, resulting in the vast majority of data being captured and generated proprietary, secured through the combinations of legal and technical restrictions (see Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Profile Books 2019; Julie E Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism, Oxford University Press 2019).

A particular challenge in terms of the use and sharing of data is the problem of advertising practices by large platforms. It has been shown that data protection alone cannot address the issues of micro-targeting, political and behavioural manipulation, nor does the GDPR provide adequate provisions for the regulation of advertising content. Collectively these practices limit users' autonomy, affect and manipulate emotions, distort election processes, and impact the rule of law. Targeted political campaigns have only deepened the debate on how to attach accountability mechanisms to actors engaged in high-risk political advertising. As they span across various regulatory and areas of law, including but not limited to constitutional and electoral laws, privacy and data protection, anti-discrimination, freedom of expression, regulation of political advertising and political parties etc., these challenges are complex. Therefore, all these areas must be considered so that a coherent regulatory framework is put in place. Limiting solutions to the regulation of digital services or competition law only will not address the myriad of other concerns and will result in more piecemeal laws and regulatory regimes. Creating a regime that focuses on interagency cooperation can also relieve some of the burden on data protection regulators.

11. What impact would the identified unfair practices can have on innovation, competition and consumer choice in the single market?

There are countless examples of the impact platform power has on limiting competition, and consequently, consumer choice and innovation. In the attention economy, users' attention is a fixed and critical resource for the advertising-funded services that make up most Internet usage. Unsurprsingly, platforms that can gain the highest percentages of attention are at a significant advantage. For example, in the UK the CMA found Google and Facebook's joint share of online user attention in the UK in April 2020 was 39% (CMA, p. 48). The European Parliament's 2019 competition report "notes with regret that one search engine that has over 92% of market share in the online search market in most of the Member States has become a gatekeeper of the Internet" (Report on competition policy – annual report 2019 (2019/2131(INI)) §40). Research company SensorTower found in May 2020 that Facebook owned four of the top ten downloaded (non-game) apps worldwide (WhatsApp, Facebook, Messenger and Instagram), while Alphabet owned two (Google Meet and YouTube) (SensorTower, Top Apps Worldwide for May 2020 by Downloads, 2 June 2020). The UK CMA also estimate that around 80% of all expenditure on search and display advertising in the UK in 2019 went to Google or Facebook. The CMA concludes*:*

'These issues matter to consumers: if competition in search and social media is not working well, this can lead to reduced innovation and choice, while poor competition in digital advertising can increase the prices of goods and services across the economy, and undermine the ability of newspapers and other providers who rely on digital advertising revenue to produce valuable content' (CMA, 2020, p. 42).

Furthermore, dominant firms are able to enter new, adjacent markets with a better advantage than their competitors. By using their knowledge of customers in one or more markets that they already dominate and by using customer information from those new markets to support their existing dominant position, "a first mover in market A can leverage

its dominant position, which comes with an advantage on user information, to let connected market B tip, too, even if market B is already served by traditional incumbent firms" (GR Barker and M Cave, Predicting and Forestalling Market Tipping: The Case of Ride-Hailing Apps in the UK, SSRN working paper, 17 January 2020, p. 9). This again results in limited competition, innovation, and consumer choice.

12. Do startups or scaleups depend on large online platform companies to access or expand? Do you observe any trend as regards the level of dependency in the last five years (i.e. increases; remains the same; decreases)? Which difficulties in your view do start-ups or scale-ups face when they depend on large online platform companies to access or expand on the markets?

Startups and scaleups largely depend on platforms to access and expand on the relevant digital markets. As indicated in examples and observations above, an increased level of dependencies has been evidenced. We have also already noted that one of the key concerns here is interoperability. We support the proposition made by the European Commission that an interoperability requirement will encourage competition, increase choice, quality for users, and the ability of competitors to provide better services (European Commission DG Connect, The Digital Services Act package, 2 June 2020).

Another obstacle to startups and scaleups is the phenomenon of "multi-homing", whereby users make use of more than one platform providing a similar service, or at least as a "partial substitute". Examples include instant messaging, and social media to some extent (CMA, 2020, p. 129). There is also an opposite issue for newcomers called 'single-homing', as a result of users' loyalty to their favourite brand or their habit (Barker and Cave, p. 13). A related concern is "tipping", the point at which one firm takes most of a market: *"driven by a combination of economies of scale and scope; network externalities whether on the side of the consumer or seller; integration of products, services and hardware; behavioural limitations on the part of consumers for whom defaults and prominence are very important; difficulty in raising capital; and the importance of brands."* (Furman et. al., p. 4). Multi-sided markets (where a platform intermediates between multiple sets of users, such as taxi drivers and passengers, or social media users and advertisers; with indirect network effects between the multiple sides of the market that are internalised by the platform) are more likely to tip when fewer users on one or more sides multi-home (Barker and Cave, p. 12).

There are also significant obstacles to the viability of new business models due to the difficulties in attracting a sufficient amount of revenues in competing with platforms. Advertising-funded platforms use current users to attract additional users and advertisers, which makes it particularly difficult for new services to compete with "free" large existing platforms. Competitors find it difficult to attract users to a new paid-for service. It is also difficult to attract advertisers to a small new platform (Crémer et al., 2019, p.20).

13. Which are possible positive and negative societal (e.g. on freedom of expression, consumer protection, media plurality) and economic (e.g. on market contestability, innovation) effects, if any, of the gatekeeper role that large online platform companies exercise over whole platform ecosystem?

We have indicated various negative effects (such as effects on democratic processes and the rule of law, media plurality, free speech, hate speech and extremism, disinformation, privacy and data protection, consumer choice, competition, autonomy, inclusion etc.).

There are also obvious political issues with democratically unaccountable private powers of historically unprecedented size. Amazon, Microsoft, Facebook, Alphabet and Apple in mid-2020 are together approaching a quarter of the value of the US's largest 500 listed

companies (Lex, Techlash: all talk, Financial Times, 14 June 2020) and their collective 2019 revenues places them between the Netherlands and Saudi Arabia, when countries are ranked by GDP (O Wallach, How Big Tech Makes Their Billions, Visual Capitalist, 6 July 2020). These companies all have headquarters in a jurisdiction with a *laissez faire* approach to regulation, or alternatively, as with Chinese giants such as Alibaba, Tencent and Baidu, the world's most populous authoritarian state.

This is a particular issue when these firms control the 'public spaces' of the Internet, where much of the social and political debate in the 21st Century occurs. While the EU has responded with frameworks like the GDPR and revamped the consumer protection regime, which applies to companies in other jurisdictions both offering goods and services to or monitoring Europeans, this cannot, on its own, address the increasingly outsized influence of tech giants on politics and everyday life.

There are some positive effects too. In many EU countries during the Covid-19 pandemic, large online platforms increasingly act as essential 'social infrastructure', used by families to share news and photos; schools to communicate with parents and students, and to teach remotely; sports teams to arrange games; politicians to communicate with constituents; campaign groups to organise protests; musicians to stream their work; and many other aspects of life.

14. Which issues specific to the media sector (if any) would, in your view, need to be addressed in light of the gatekeeper role of large online platforms? If available, please provide additional references, data and facts.

Traditional media, broadcast, cable, and satellite TV and radio distributors, are required in many European countries to carry specified channels, and to give prominence in electronic programme guides to certain channels, both to widen the distribution of public service broadcast content, and to protect media pluralism and diversity (L Woods, Must Carry/Must Offer obligations on audiovisual services under EU Law, Harbottle & Lewis Insights, 20 December 2019). These types of requirements are yet to be extended to major online platforms. The US Stigler report concluded that interoperability "may contribute to reducing the gatekeeping power of [dominant] platforms and positively impact the type of information that users consume." (Stigler Committee on Digital Platforms, Final Report, September 2019, p. 144).

A 2020 report from Germany's National Academy of Science and Engineering called for a "European digital ecosystem that is democratically accountable to its citizens. A digital ecosystem that observes European values such as transparency, openness and privacy protection, even in its technical design, can create a digital public sphere that offers fair terms of access and use, strengthens the public debate and safeguards the plurality that forms a key part of Europe's identity." The report identified the importance of this goal of "a technology strategy characterised by modularity, interoperability, openness and transparency that enables continuous development and a diverse range of business models." (H Kagermann, U Wilhelm (Eds.) European Public Sphere: Towards Digital Sovereignty for Europe, Munich: acatech – National Academy of Science and Engineering, 2020). We agree and call for embedding these principles in the upcoming regulatory regime for platforms in the EU.

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

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

In summary, this cooperation has been mostly inconsistent, insufficient and uncoordinated and despite empowerment to do so, a woeful lack of enforcement. The problem is, as noted above, that different regulatory regimes do not address concerns around platforms in a coherent and coordinated manner. Thus, we see legislation and regulation enforced often in silos of areas such as competition law, electronic communications, consumer protection, data protection, media regulation, intellectual property. These tasks are, understandably, placed in the hands of different regulators who do not have capacities or mechanisms to coordinate their enforcement actions and other regulatory tasks. There is also a sense that data protection regulators refuse to engage in meaningful dialogue with their counterparts in other regimes. Even within a specific sector, there is an issue with cross-border cooperation. The problem is exacerbated when translated to establishing cooperation between various sectoral regulators. There have been some good attempts to foster cooperation in data protection under the GDPR requirement, but even this has proven insufficient. Another key issue here is different 'regulatory power' between member state's regulators, which result from different funding capacities, member state size and resources, regulatory independence, etc. Lastly, there is a problem with conflict over regulatory competences; for example, the EU's data protection regime regulates the processing of personal data when necessary for the performance of a contract. However, the consumer protection regime also has well-established principles regarding what amounts to (un)fairness in contracts and the pre-contractual environment, yet the data protection regime appears to be unwilling to cooperate with its consumer protection counterparts.

4. What information should competent authorities make publicly available about their supervisory and enforcement activity?

Regulators must adhere to transparency requirements themselves, in particular, regarding their funding. Provisions for alternative views on the complaint should be permitted and encouraged. For example, European and national regulators exist to protect the fundamental right to data protection, yet there is no equivalent protection for free expression or other digital rights. Complaints from business and enterprise should be adequately investigated, but views should also be sought from consumer protection organizations and civil society beyond those regulators who have a narrow scope of interest like media authorities. The regulator should also encourage views from users or help to establish user collectives to allow their opinions to be given standing.

The regulators should monitor institutions and organisational efforts to educate and raise awareness. The regulator should require periodic reports on the effectiveness of these activities and ensure organisations reach the general public each time a new technological tool, service or product is developed. This will help to ensure that the general public remains educated on how to safely use new products and services. We support the introduction of Child Safety Impact Assessments to be filed with the regulator every time a company designs an online service or product marketed at children.

In addition to the information they already provide, regulators should also make available information about various existing and future types of impact assessment. Examples include DPIAs, but also human rights impact assessment, child protection impact assessments, ethical/societal impact assessments for all products and services, including retroactively.

5. What capabilities – type of internal expertise, resources etc. - are needed within competent authorities, in order to effectively supervise online platforms?
Competent authorities need to be equipped with expertise in various areas of law, economics (in particular behavioural), technology, social sciences (especially cognitive and social psychology) and humanities. Given all the concerns we mention, internal expertise needs to be interdisciplinary so that the regulator is capable to identify and address issues holistically. This is, of course, complex and challenging given the budgetary limitations in member states, the lack of human resources and expertise available to certain regulators etc. Thus, cross-border cooperation is crucial. Furthermore, s better-resourced regulators should support those with more limited capacities.
The regulator should not have the power to disrupt the business, as this should be placed into the hands of judicial authorities, if absolutely necessary. Generally, we would not recommend going much beyond the current powers different regulators have, but only for illegal content. Senior management liability could be implemented for intentional or negligent, large scale breaches and offences (e.g. manipulation and political advertising, hacking, data misuse scandals etc.), making sure that there are appropriate appeals procedures. For example, we suggest adopting the use of enhanced certification procedures as in the GDPR. This should also be included in the revised text of the e-Privacy Regulation.

8. How should the supervision of services established outside of the EU be set up in an efficient and coherent manner, in your view?
Given the number and the relative dominance of these services, cooperation between sectoral and member states regulators is crucial. Platforms should not be allowed to 'forum shop' and regulators in member states where the main establishments of large companies are based should be offered support by a coordinating pan-EU regulator/supervisory mechanism. This would help address the reality of regulators in smaller members states not having the adequate resources adequately to respond to large companies with vast expertise and budgets. Ideally, this should not just be a task for the Europen Commission, BEREC, EDPB or the Consumer Protection Authorities, but there is room to establish a body that will coordinate collaboration and work between different sectoral regulators as well as national regulators.

9. In your view, what governance structure could ensure that multiple national authorities, in their respective areas of competence, supervise digital services coherently and consistently across borders?
We need enhanced collaboration, pan European (meta) as well as future thinking regulators/supervisors and support for under-resourced national regulators. Importantly, there is a need for harmonisation, or at the very least, an approximation of national institutional and procedural rules to set up a more efficient common liability online regime applicable across the EU.

Regulation of large online platform companies acting as gatekeepers
1. Do you believe that in order to address any negative societal and economic effects of the gatekeeper role that large online platform companies exercise over whole platform ecosystems, there is a need to consider dedicated regulatory rules?
Fully agree
2. Please explain

3000 character(s) maximum

At present the rules for regulating gatekeepers are disparate and challenging to comprehend and apply to every situation that could result in harmful societal and/or economic effects. As discussed in a previous section, to exacerbate matters, content regulation for online advertising is absent from the European regulatory *acquis*. Neither the consumer protection regime nor the specific purpose limitation principle in the EU's data prtotection regime is *prima facie* ripe for the regulation of racist and hateful content that appears in advertising. Under the current regime, gatekeepers are solely responsible for assessing the content of malicious and advertising content. Importantly, the power of gatekeepers' ecosystems for shaping individual actions and facilitating the scaling up of those actions to notable changes in collective behaviours is that minor technological revisions can result in significant changes. For instance, curtailing the number of times a message can be forwarded on WhatsApp (thereby slowing large cascades of messages) may have contributed to the absence of lynch killings in India since 2018. This specific regulatory action does not fit neatly into the consumer nor the data protection regime (Freitas Melo, 2019), yet achieves the desired outcome.

Establishing causality between the harms associated with gatekeep power is crucial because it offers opportunity for intervention and regulatory action. If gatekeepers were found to cause societal ills, then it would be legitimate to expect that a change in choice architecture might influence society's well-being. Absent causality, this expectation does not hold: For example, if one group of people were particularly prone to express their hostilitities through anti-social behaviours and by hostile engagement, then any intervention targeting gatekeepers would merely prevent one expression of an underlying problem while leaving the other unaffected.

Data protection does not regulate the attention economy, nor is it designed to. Its scope is limited to the processing of personal data. Consumer protection is only designed to protect consumers, not users. Neither are place to properly regulate choice architectures which are persuasive and manipulative *in themselves,* and can steer online behavior in a the service of commercial interests (e.g. 'dark patterns', privacy-intrusive default settings (Leiser 2020)) or in political directions through algorithmic content curation (e.g. targeted advertising, personalised recommender systems, algorithmic filtering in search engines, personalized curation of news feeds on social media (Leiser, 2021)). These methods are particularly troublesome when online content not based in factual knowledge and that misleads the public by instilling inaccurate beliefs and/or undermining trust in legitimate media sources.

As the scope of data protection is limited in the material sense and the scope of consumer protection is limited in the personal sense, the European Union's frameworks for the protection of consumers and data subjects is not sufficient. Moreover, there is a troubling trend among data protection regulators to develop convulted interpretations of the law in order to fix perceived problems associated with advertising and marketing. Not only does this prove challenging for the rule of law, but undermines the legitimacy of the regime, creates confusion for businesses operating in the digital single market and weakens protection available to users.

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

4. Please explain your reply and, if possible, detail the types of prohibitions that should in your view be part of the regulatory toolbox.
3000 character(s) maximum
One of the great legislative successes of the European Union's Consumer Protection Regime is the structure of the Unfair Commercial Practices Directive. This requires a breach of 'professional diligence' and a 'material distortion' of a consumer's decision. This is very broad and depends on the national interpretation of 'professional diligence' with the circumstances analysed on a case-by-case basis. Articles 6 and 7 contain provisions about misleading omissions and actions. There must be an omission or misleading presentation of information and which results in the material distortion of the consumer's decision. In order for a practice to be considered aggressive under Article 8, there must be an element of an aggressive practice like undue influence and material distortion of the consumer's decision. The Directive also contains an Annex of blacklisted items. Once the practice described in the Annex is proved, there is no need to prove that the practice resulted in a material distortion. The prohibition of certain practices should be tied to harms to *users*, as opposed to *data subjects* and/or *consumers*. This ensures that there are benchmarks for acceptable and reasonable business and advertising practices alongside a blacklist of practices that harm users that can be easily added to over time. This can also address a number of the child protection issues identified in a previous section of this submission. In a significant departure from the method deployed in the UCPD, all users should be presumed *vulnerable* to ensure a high level of protection and a healthy digital ecosystem. The prohibitions should, therefore, begin with what is unacceptable for a child and not rely on what amounts to an *average* user.
Certain advertising practices that are presently largely unregulated in the present ecosystem could be easily added to a blacklist of prohibited practices in any circumstances. For example, political microtargeting, using personal data to make political inferences, failing to register as a political advertiser during an electoral event, AstroTurfing, malicious content, unregistered AI, failing to conduct publically auditable impact assessment(s), operating a careless and malicious data brokerage are all examples of the type of behaviours that could be outlawed under a new regulatory structure.

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

6. Please explain your reply and, if possible, detail the types of obligations that should in your view be part of the regulatory toolbox.
3000 character(s) maximum
One of the pressing issues for gatekeepers is accountability beyond the mechanisms that are applicable to those within the European Union. Accordingly, the new regime should include certification requirements for any platform operating a business directed at EU users. An obligation of personal liability for gatekeeper directors should be enshrined into

law. Any advertiser undertaking an business or advertising practice identified by a regulator as high risk (for example, issue-based advertising) should undertake an publically auditable impact assessment (ensuring *ex-ante* compliance) and make their content subject to scrutiny in a repository of advertisements alongside additional information about which users were served what content and when.* Beyond the repository of advertisements, users should be able to determine what psychological attributes were used in the microtargeting of advertisements and what reinforcement architectures (if any) were deployed to prompt users to constantly 'refresh' their feeds and check their devices. Furthermore, any gatekeeper should be subjected to an independent human rights audit by a panel chosen by an independent regulator to ensure compliance with standards, *ex-post*.

*It is also BILETA's opinion that one cannot achieve a healthy digital ecosystem without meaningful reform of corporate goverance and widening shareholder lawsuits to hold directors to account for their specific consideration of the imact of their data collection and processing and online behavior (including manipulative and harmful business practices).

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

Yes

8. Please explain your reply.

3000 character(s) maximum

Yes, not every issue affects someone's interests as a data subject, nor does everyone qualify as a consumer in order for the consumer protection regime to activate. Furthermore, while some civil society organisations specialise in either, children, technology, and/or Internet policy, they typically do not have the capacity to participate broadly, nor are they necessarily representative of the larger Internet community. Nevertheless, understanding of user(s) needs is profound, and are the best informed advocates for concerns; a new regulator/authority should be considered a primary channel for engaging the broader Internet community beyond data and consumer protection. A promising approach to help fill these gaps is to identify and engage with specifically affected communities when making decisions that might affect them; for example, one or more industry associations, user groups, or a set of individuals (on network communitarianism, see Murray 2008).

Of course, users are diverse and the ability of a limited number of agents to properly represent individual interests is imperfect, but this arrangement is an improvement over the alternative. Putting the 'user' in the heart of a new regulatory authority creates a virtuous cycle; it allows multiple implementations, allows users to seek a remedy with relatively low costs and creates an incentive for gatekeepers, including platforms and advertisers to carefully consider the users' needs, which often are reflected back into the definition of new standards. The resulting ecosystem may have many remaining problems, but the creation of a new 'user'-centric regulator provides an opportunity to improve it and lead in response to the numerous calls for further interagency cooperation and reliefs some of the pressure from the problematic, if not failing, data protection enforcement regime.

Furthermore, this new regulator should unambigiously build a better digital ecosystem. Not only will the work not be collared by the limitations of definitional scope that plague the data and consumer protection regimes, users with an interest in a particular issue can 'tussle' for the best approach to a specific problem.

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

10. If yes, please explain your reply and, if possible, detail the types of case by case remedies.
3000 character(s) maximum
Yes, platforms are large, publically traded companies subject to corporate governance rules and well-established mechanisms for shareholders to hold directors accountable for their leadership and decisions. Accordingly, there should be a range of remedial mechanisms that can be used on a case-by-case basis that can apply to a wide-range of behaviours and harms. As the market can absorb and internalize any possible penalties for bad behaviour, there should be no caps on financial penalties for when a gatekeeper has undertaken a systematic and prolific business practice to the detriment of the entire digital ecosystem. At the other end of the spectrum, an injunction or interdict should be available to require a business from undertaking a specific practice. Alternative remedies like revoking a license to operate in the European Union alongside blocking injunctions that can be applied at backbone level across the EU should be used as part of a carrot-and-stick approach to platform enforcement.
11. If you consider that there is a need for such dedicated rules, as referred to in question 9 above, do you think there is a need for a specific regulatory authority to enforce these rules?
Yes
12. Please explain your reply
3000 character(s) maximum
Please see the reply to Question 8 above.

13. If you consider that there is a need for a specific regulatory authority to enforce dedicated rules referred to questions 3, 5 and 9 respectively, would in your view these rules need to be enforced by the same regulatory authority or could they be enforced by different regulatory authorities? Please explain your reply.
3000 character(s) maximum
It is not necessary or desirable to have one regulator informing other regulators of how to do their job and how to enforce regulations. Accordingly, the new proposed regulatory authority should be empowered to enforce **new hybrid form of** regulation to protect both individual users and the societal harms from excessive and abusive gatekeepers. In addtion to principle-based rules, there should be a blacklist of certain practices that should not be permitted in any circumstances. Furthermore, the regulator can influence interpretation of existing rules in conjunction with different, existing regulatory authorities through this form of principles-based regulation which is focused on achieving the right outcomes is desirable in the fast-changing digital world. This generality allows the approach to work across different types of regulation and authorities and would be largely future-proof. A principle-based system of regulation aligns with existing principles anc can act as a 'source of continuous learning: drawing on relevant measures to identify lessons for improving the mechanism and preventing future grievances and harms'. A blacklist of practices can also evolve with the fast-paced changes in digital technologies.

14. At what level should the regulatory oversight of platforms be organised?
Both at EU and national level.

15. If you consider such dedicated rules necessary, what should in your view be the relationship of such rules with the existing sector specific rules and/or any future sector specific rules?
3000 character(s) maximum
In addtion to principle-based rules, there should be a blacklist of certain practices that should not be permitted in any circumstances. Furthermore, the new regulator can influence interpretation of existing rules in conjunction with different, existing regulatory authorities through this form of principles-based regulation which is focused on achieving the right outcomes is desirable in the fast-changing digital world. For example, a regulatory obligation to undertake an impact assessment of the practice could premptively be applied in situations where there are reasonable concerns that a gatekeeper's activity could cause harm, but the scale and risk of these issues is unproven. The onus of an practice impact assessment moves to an organisation to prove that their practices are safe and to a reasonable level. This generality allows the approach to work across different types of regulation and authorities and would be largely future-proof (Ruggie's Guiding Principles on Business and Human Rights).
A supplementary blacklist of practices can also evolve with the fast-paced changes in digital technologies. Additional sector-specific rules can be adopted far more quicker than a general regulation can evolve to regulate new practices and/or digital technologies.
16. Should such rules have an objective to tackle both negative societal and negative economic effects deriving from the gatekeeper role of these very large online platforms? Please explain your reply.
3000 character(s) maximum
Yes, this is self-evident from the answers already provided above – as long as it the rules and the objective also align with the protection of other fundamental rights as well.
17. Specifically, what could be effective measures related to data held by very large online platform companies with a gatekeeper role beyond those laid down in the General Data Protection Regulation in order to promote competition and innovation as well as a high standard of personal data protection and consumer welfare?
3000 character(s) maximum
Earlier in this submission, BILETA's reiterated the case for interoperability among platform Beyond interoperability, we would like to see the data portability rules extended to cover grounds beyond consent and for the performance of a contract. Further regulation is needed of, although not strictly online platform companies, data brokers and data brokerages. Further information about advertising should be obligated to held in public repositories. Transparency obligations should be applicable to inferences made and access obligations to shadow profiles. Data shared across systems and services, which curtails the ability of users to understand what can be inferred from their data and what they might be disclosing about others. One example of the complexity of digital privacy is the possibility to build shadow profiles with information on individuals who do not have a platform account (). Information on these individuals can be inferred from the data that users voluntarily provide, which can be combined with contact lists and other kinds of relational data to make inferences of personal attributes of people without an account. This inference builds on statistical patterns of social interaction, leading to for example, the assortative mixing of

personal attributes like political affiliation or sexual orientation (). When empirical data on social networks are combined with simulations of the spreading of their adoption, it can be illustrated how a network can infer the friendship between two non-users. Accordingly, shadow profiles, inferences, and certain ML-modelling should be brought under the umbrella of a new regulator.

18. What could be effective measures concerning large online platform companies with a gatekeeper role in order to promote media pluralism, while respecting the subsidiarity principle?

3000 character(s) maximum

N/A

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

Institutional cooperation with other authorities addressing related sectors – e.g. competition authorities, data protection authorities, financial services authorities, consumer protection authorities, cyber security, etc.

Pan-EU scope

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

Capacity building within Member States

High level of technical capabilities including data processing, auditing capacities

Cooperation with extra-EU jurisdictions

20. There is no Question 20 on the PDF Questionaire.

21. Please explain if these characteristics would need to be different depending on the type of ex-ante rules (see questions 3, 5, 9 above) that the regulatory authority would be enforcing?

3000 character(s) maximum

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

Reporting obligation on gatekeeping platforms to send a notification to a public authority announcing its intention to expand activities

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

Investigative powers for the public authority

Other

23. There is no Question 23 on the PDF of the Questionaire.

24. Please explain if these requirements would need to be different depending on the type of ex ante rules (see questions 3, 5, 9 above) that the regulatory authority would be enforcing?

3000 character(s) maximum

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

See Chart and the highlights therein sent in a different PDF for suggestions

26. Please explain which of the options, or combination of these, would be, in your view, suitable and sufficient to address the market issues arising in the online platforms ecosystems.
3000 character(s) maximum

27 Are there other points you would like to raise?
3000 character(s) maximum
N/A

Part VII: Governance of digital services and aspects of enforcement
10. As regards specific areas of competence, such as on consumer protection or product safety, please share your experience related to the cross-border cooperation of the competent authorities in the different Member States
3000 character(s) maximum

11. In the specific field of audiovisual, the Audiovisual Media Services Directive established a regulatory oversight and cooperation mechanism in cross border cases between media regulators, coordinated at EU level within European Regulators' Group for Audiovisual Media Services (ERGA). In your view is this sufficient to ensure that users remain protected against illegal and harmful audiovisual content (for instance if services are offered to users from a different Member State)? Please explain your answer and provide practical examples if you consider the arrangements may not suffice.
3000 character(s) maximum

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

13. Other areas of cooperation - (please, indicate which ones)

14. Are there other points you would like to raise?
3000 character(s) maximum
N/A