EDRi response to the European Commission's open public consultation on the Digital Services Act package

19 August 2020

I. How to effectively keep users safer online?

1. Main issues and experiences

A. Experiences and data on illegal activities online

Questions 1.-19.: no EDRi response

20. 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)? 3000 character(s) maximum

Misleading advertising is poorly handled by major online platforms. In June 2018, Facebook announced it had created a compulsory "Paid for by" feature that is supposed to require advertisers to submit a valid ID and proof of residence before they are able to spread ads. The feature was introduced as a reaction to a series of misleading or false political and issue-based online ads on Facebook that were paid for by foreign actors with the aim of influencing domestic democratic elections. The feature was supposed to help reduce the sales of misleading ads and help fight election manipulation and online disinformation. Since then, several independent experiments have been conducted to see whether ad manipulation is still possible on Facebook. Facebook failed all these tests.

For example, in October 2018, journalists were able to pose as politicians, the Islamic State as well as all 100 US senators, and post and sponsor political ads on Facebook under fake identities. The low quality of Facebook's screening process allowed tricking the system without any specific technical knowledge (https://www.vice.com/en_us/article/xw9n3q/we-posed-as-100-senators-to-run-ads-on-facebook-facebook-approved-all-of-them and https://www.vice.com/en_us/article/wj9mny/facebooks-political-ad-tool-let-us-buy-ads-paid-for-by-mike-pence-and-isis).

More recently, British consumer protection organisation "Which?" revealed how fraudsters can create scam Facebook and Google ads within hours due to a crucial lack of effective controls (see https://press.which.co.uk/whichpressreleases/fraudsters-can-create-scam-facebook-and-google-ads-within-hours-which-reveals).

In 2020, EDRi member Metamorphosis Foundation in Macedonia warned against scammers using fake Forbes articles and anti-EU disinformation as bait to target Facebook users across Europe. It took several weeks for Facebook to remove the ads reported as scams. Read more here: https://edri.org/cryptocurrency-scammers-flood-facebook-users-with-manipulative-ads.

The examples show that major platforms are not properly controlling their ad admission processes. Whether this is due to a lack of capabilities or willingness is hard to prove. Looking at the business incentives for ad-driven platforms, however, it seems likely that the identity verification for advertisers is failing on purpose. Every blocked ad represents missed profits. Or as the former Head of Global Elections Integrity Ops at Facebook, put it: "The real problem is that Facebook profits partly by amplifying lies and selling dangerous targeting tools that allow political operatives to engage in a new level of information warfare. [...] As long as Facebook prioritizes profit over healthy discourse, it can't avoid damaging democracy" (see https://www.washingtonpost.com/outlook/2019/11/04/i-worked-political-ads-facebook-they-profit-by-manipulating-us).

21. Do you consider these measures appropriate?

Yes

» No

I don't know

22. Please explain. 3000 character(s) maximum

The use of automated detection tools to address risks for people and societies to be exposed to misleading ads, scams and other unfair practices does not work and there are risks that the systems misidentify fair and legitimate practices/content. See EDRi's responses on political online advertising below.

B. Transparency

Questions 1.-4.: no EDRi response

5. When content is recommended to you - such as products to purchase on a platform, or videos to watch, articles to read, users to follow - are you able to obtain enough information on why such content has been recommended to you? Please explain. 3000 character(s) maximum

Most platforms provide very limited information about the reasons for which they display certain content to certain users but not to others. Despite attempts by a few companies to introduce transparency mechanisms (such as Facebook's transparency and control tools, including the "Why I'm Seeing This Ad?" feature), this remains mostly opaque for average users, researchers and public authorities.

It is mostly unclear how ads are optimised to reach the targeted audience and to trigger a reaction, a process that entails sophisticated data science/machine learning models that are unknown to and unverifiable for users. Users should be able to know at least:

- If a political advertiser used the custom audience tool, and if so, if an email address was uploaded,
- What "look-alike audience" advertisers, who are trying to find other users with similar data as their original targets, are seeking,

- The true, verified name of the advertiser and who paid for the ad,
- How Facebook's algorithms amplified the ad.

Transparency and other measures ensuring user control should guarantee the full access to one's personal data. Users should be able to control the content they interact with by being allowed to filter out what they do no want to see. Users of platforms with significant market power should also be able to decide if they want to receive algorithmically-curated recommendations at all via an opt-in/opt-out mechanism.

EDRi member Panoptykon Foundation found in a recent study about online political advertising that users do not currently have control over their marketing profiles and cannot verify true reasons for being included in a particular target audience. The study develops policy recommendations for regulating online intermediaries and advertisers: https://panoptykon.org/political-ads-report.

Ads and content recommendations are usually also based on intimate browsing data from users collected via tracking pixels and embedded code on third-party websites ("Like", "Share", or "Tweet" buttons) but also via embedded Youtube videos, Instagram posts, and even WhatsApp chats.

EDRi member Electronic Frontier Foundation recently published a detailed report on the technical methods and business practices behind the collection of personal information by corporate third-party trackers, and unveils the scope of their activities (see https://www.eff.org/wp/behind-the-one-way-mirror).

EDRi member Privacy International found that Facebook even collects personal information about people who are logged out of Facebook or don't even have a Facebook account. The company owns so many different apps, "business tools" and services that it is capable of tracking users, non-users and logged-out users across the internet (see https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report).

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

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

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

On many online platforms, however, including those built for them, children are not sufficiently protected against privacy intrusions and data exploitation. Today's children have the biggest digital footprint of any generation in human history. Sometimes, the collection of a child's data starts even

before they are born, and this data will increasingly determine their future (https://www.unicef.org/child-rights-convention/open-letter-to-worlds-children#digital). Third parties that record children's every step not only increase the risk that past actions may later be used against them, but it exposes them to early commercial and political manipulation through micro-targeted advertising (https://www.ugent.be/re/mpor/law-technology/en/research/childrensrights.htm).

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

A Big Brother Watch 2018 report found that the UK "demands a huge volume of data about individual children from state funded schools and nurseries". Data such as a child's name, birth date, ethnicity, school performance, special educational needs and so on, are easily combined with other publicly available information. Local authorities are working with tech giant IBM to train algorithms that predict children's behaviour in order to identify children prone to gang affiliations or political radicalisation. But algorithms portray human biases, for example against people of colour. Reports show that authorities treat children in danger to be recruited by a gang as if they were part of the gang already. Therefore, racial profiling by algorithms can turn into a traumatic experience for a child (https://www.theguardian.com/society/2018/sep/17/data-on-thousands-of-children-used-to-predict-risk-of-gang-exploitation and https://www.independent.co.uk/news/education/education-news/teachers-forced-to-act-as-front-line-storm-troopers-to-spy-on-pupils-under-guidelines-aimed-at-10158043.html).

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

	Fully agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Fully disagree	Idk/No reply
Online platforms can easily be manipulated by foreign governments or other coordinated groups to spread divisive messages						X
To protect freedom of expression online, diverse voices should be heard	X					
Disinformation is spread by manipulating algorithmic processes on online platforms						X
Online platforms can be					X	

trusted that their internal practices sufficiently guarantee democratic integrity, pluralism, non-discrimination, tolerance, justice, solidarity and gender equality.						

3 Please explain. 3000 character(s) maximum

Freedom of expression is not only about protecting information or ideas that are "favourably received or regarded as inoffensive", but also about protecting those that "offend, shock or disturb the State or any sector of the population" (ECHR 5493/72). It is important that restrictions of speech are strictly limited to what is necessary and proportionate and criminal law is not an appropriate tool to fight disinformation at scale and it creates a dangerous space for human rights abuse in the form of state-sponsored intimidation and unjustified prosecution of dissenting voices.

Of course private platform operators can search for, tag or remove disinformation, "inauthentic behaviour", and related user accounts on their system. But rather than focusing legislative efforts on the removal of inaccurate content online, the DSA should aim at reducing the incentive for ad-driven platforms to spread disinformation and divisive content. The danger of online disinformation lies in its systematic (and often paid-for) viral spread across centralised, closed platforms. As long as that commercial incentive exists, online platforms cannot sufficiently guarantee internal practices that promote democratic integrity, pluralism, non-discrimination, tolerance, justice, solidarity and gender equality.

The DSA can approach this problem in several ways:

1. At a minimum, the current cookie wall practice needs to stop. If properly enforced, existing laws would already prevent the use of personal data for ads without consent. By restricting targeted ads and algorithmic recommendation, platforms would lose the incentive to collect personal data in the first place which in turn would remove the financial incentives to spread disinformation and and divisive content.
2. The DSA could prohibit advertisers from targeting users with content based on very sensitive personal data like psychological profiles, political opinions, sexual orientations, or health status. This limitation should include all types of content, political, issue-based, commercial, or otherwise. This would not impede online advertising: publishers, bloggers, app developers, and others can still use generic or contextual ads to generate revenue without collecting any data about users.
3. Lastly, the DSA should empower users to choose the content they want to interact with and the platforms they really want to be on. At the moment, billions of users cannot escape the small handful of powerful centralised mega platforms without losing all of their online contacts. In other words, everybody is on WhatsApp or Facebook not because these are the

best platforms imaginable, but because everybody else is there. The DSA should therefore mandate dominant platforms to allow interoperability with competitors so that users can switch and still communicate across platforms. The DSA should further promote the ability of users to delegate some services (i.e. content moderation) to competing service providers, if they so choose.

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

The COVID-19 pandemic has created new topical opportunities for those seeking to spread hate speech and disinformation online. It has not, however, caused any structural changes to how disinformation works or should be tackled. COVID-19 should therefore not be used as a pretext to tighten rules on content removal or other rights-infringing legislative approaches. Implementing the suggestions in our answer to question 1.C.3 above in the DSA would go a long way in reducing the potential harms that disinformation around COVID-19 can cause. For details on dos and don'ts with regards to the COVID-19 response, please see EDRi member Access Now's dedicated recommendations on "Fighting Misinformation And Defending Free Expression During Covid-19" at https://www.accessnow.org/cms/assets/uploads/2020/04/Fighting-misinformation-and-defending-free-expression-during-COVID-19-recommendations-for-states-1.pdf.

Question 5.: no EDRi response

D. Experiences and data on erroneous removals

This section covers situation where content, goods or services offered online may be removed erroneously contrary to situations where such a removal may be justified due to for example illegal nature of such content, good or service (see sections of this questionnaire above).

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

Unfortunately, platform providers do not collect or share comprehensive data about the scale and impact of wrongful content removals or account bans and there is, for the time being, no legal requirement for platforms to publish such data. Without this information, it is impossible to know what kind of regulatory action is necessary and what kind of action on the side of platforms are working or not working well.

This is why the DSA should introduce an obligation for platforms to regularly publish data about content takedowns, account bans, appeals procedures and content reinstatements—in a harmonised way that allows comparison between different platforms. At the moment, researchers, policymakers, NGOs and the general public must rely on the companies' good will, individual reporting and press stories as well as independent, community-led initiatives to document platforms' impact on people's free speech. In addition, the DSA should at least promote the reinstatement of wrongfully deleted or disabled online content in order to protect users' freedom of expression.

We have collected a few examples for the purpose of this consultation to highlight the nature of the problem:

- In 2019, Facebook for the first time released statistics about the appeals it received on content takedowns. The report showed that in the first quarter of 2019, Facebook restored more than 80,000 posts that were mistakenly removed as harassment and over 130,000 pieces of content that were incorrectly flagged as hate speech. In its latest report covering the period of January-March 2020, Facebook's affiliate, Instagram, reported that out of 53,400 appealed content takedowns allegedly picturing child nudity and sexual exploitation of children, almost 30% of content was reinstated. This amounts to 16% of all removed content from this category (not an insignificant number considering that this category of content is often portrayed as "manifestly illegal" and therefore easy-to-spot..)
- On copyright infringements, our member EFF collects in its hall of shame the worst cases of wrong copyright and trademark complaints: https://www.eff.org/takedowns
- Counter-speech and precious evidence of human rights violations in dictatorships are being deleted by "anti-terrorism" and "anti-extremism" filters: https://www.eff.org/wp/caught-net-impact-extremist-speech-regulations-human-rights-content
- A 2019 report by Salty, an online community for voices of women, trans and non-binary people, found that queer people and women of colour are policed at a higher rate than the general population. Plus-sized profiles were often flagged for "sexual solicitation", and policies introduced by platforms to protect users from racist or sexist behaviour are harming the very groups that need protection. Moreover, the high number of accounts that are reinstated after wrongful deletion indicates that there is a high rate of false flagging. The report also criticises the opaque appealing process put in place by most online platforms (see https://saltyworld.net/algorithmicbiasreport-2).

Other sources of information are provided by third parties, often civil society groups trying to measure the scale of the problem we are facing. They include "Onlinecensorship.org", a project of EDRi member Electronic Frontier Foundation which addresses the lack of recourse for content takedowns by providing a platform where users of social media sites can report erroneous takedowns. It also documents censorship trends affecting specific communities: https://onlinecensorship.org/

Similarly, the recent project "Silenced Online" runs both a platform to crowdsource user reports on content takedowns and a campaign to raise awareness about companies' content moderation policies and their biases in enforcing platforms' community guidelines: https://silenced.online/about.

Questions 3.-7.: no EDRi response

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

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

Yes, specific data, requested as a competent authority

Yes, through bilateral or special partnerships

On the basis of a contractual agreement with the platform

» Yes, generally available transparency reports

Yes, through generally available APIs (application programme interfaces)

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

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

Yes, other. Please specify in the text box below

No

9 Please indicate which one(s). What data is shared and for what purpose, and are there any constraints that limit these initiatives? 3000 character(s) maximum

As a digital rights organisation, EDRi is searching for data about the appearance of potentially illegal online content and activity as well as the way that online platforms are dealing with it. Namely, we seek data about:

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

Some of this data can be found in some of the platform companies' reporting. However, most of this type of data is not published at the moment. If it is, it is through non-structured claims rather than raw data that researchers and oversight authorities can work with.

That is why the DSA should introduce mandatory publication of such data for all large platform operators in a machine-readable pre-defined format. Only then will we be able, as a society, to truly understand the extent to which online platforms contribute to and influence our public debates, how

they potentially manipulate people's thinking and pre-determine what individual's read or don't read online.

Questions 10.: no EDRi response

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

» Yes

No

I don't know

12. Please specify for what specific purpose and if the information available to you sufficient, in your opinion? 3000 character(s) maximum

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

13 How valuable is this information for you?

The information currently contained in the WHOIS database is valuable and sufficient.

14. Do you use or are you aware of alternative sources of such data? Please explain. 3000 character(s) maximum

No.

Section 1.: no EDRi response

The following questions are open for all respondents.

2. Clarifying responsibilities for online platforms and other digital services

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

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

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

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

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

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

- The name and contact details of the notifying party in cases only where this is necessary to process the notice;
- The link (URL) or – if there is no URL for technical reasons – a similar unique identifier to the allegedly illegal content in question;
- The stated reason for the complaint including, where possible, the legal basis the content in question is allegedly infringing;
- Depending on the type of content, additional evidence for the claim; and
- Where a complaint is not anonymous, a declaration of good faith that the information provided is accurate in cases of copyright infringement and defamation cases.

Other, please specify

4 Please explain, 3000 character(s) maximum

The URL or similar identifiers are necessary to enable platform providers to unmistakeably identify the content that is alleged to be illegal. A notification should be easy to make for non-experts, yet it should require sufficient thought process from the notifying party to discourage mass false notification. Therefore a stated reason/explanation and, where applicable, supporting evidence (rather than a formal legal argument) should be included in any notification.

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

The best solutions will depend on the type of platform: Preventing the reappearance of illegal content on content hosting platforms (like social networks, video sharing, micro-blogging or similar systems) require different approaches than online marketplaces that sell goods and services. This is because contrary to marketplaces, any regulation of content hosting intermediaries has strong freedom of speech implications.

While it can be a good idea to require online marketplaces to (automatically or manually) check every single uploaded offer of goods or services before it appears on the site, this cannot be appropriate for content hosting platforms where such prior restraints of content would lead to inappropriate limitations of the freedom of expression protected under EU fundamental rights law. This does of course not prevent content hosting platforms from deciding to operate such checks voluntarily and they are free to use the solution they see fit (machine learning algorithms, simple hash databases, file name checks…). But no law should *oblige* platform providers to use such technologies. Instead, content removal, including the problem of reappearing illegal content, should be addressed through judicial due process.

6 Where automated tools are used for detection of illegal content, goods or services, what opportunities and risks does their use represent as regards different types of illegal activities and the specificities of the different types of tools? 3000 character(s) maximum

The use of automated tools for the detection and removal of illegal content should never be mandated by law.

Online platforms overly relying on the use of automated identification and removal tools tend to record higher rates of wrongful take-downs. Algorithms perform badly at understanding and assessing the context in which content is produced, notably cultural, linguistic and social norms. Even in straightforward cases, they make false matches.

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

Because of their contextual blindness or, in other words, inability to understand users' real meaning and intentions, automated tools often flag and remove content that is completely legitimate. Thus, journalists, activists, comedians, artists, as well as any of us sharing our opinions and videos or pictures online risk being censored because internet companies are relying on these poorly working tools.

In another striking example, as the COVID-19 crisis broke out, health guidelines forced big social media companies to send their content moderators home. Facebook's automated "anti-spam" system kicked in and – just like on other social media platforms – started removing crucially important information about the pandemic from trustworthy sources as violations of the platforms' community guidelines. This period perfectly demonstrates why relying on automated processes is often detrimental to the freedom to receive and impart information and democratic debates and processes and should therefore not be required by law.

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

a. Digital services established outside of the Union?

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

Questions b.: no EDRi response

8 What would be appropriate and proportionate measures that digital services acting as online intermediaries, other than online platforms, should take – e.g. other types of hosting services, such as web hosts, or services deeper in the Internet stack, like cloud infrastructure services, content distribution services, DNS services, etc.? 5000 character(s) maximum

Intermediaries that do not host but only cache or transmit user-uploaded content (such as DNS services, cloud fronting services and peer-to-peer messaging services for example) should not be held responsible for the content they transport.

Web hosts, CDNs and other cloud storage providers that do host user-uploaded content should only be held liable for that content if they refuse to act upon a valid court order in which content stored

on their system has been declared illegal. They should not be held liable for failure to pro-actively search for or remove content that has not been declared illegal by the courts. Platform operators are not the judiciary. Giving them the power (or creating a legal obligation for them) to behave as if they were the judiciary (a) undermines the institutional and legal order of our democracy, and (b) cements the quasi-monopolistic position that many of these platform operators already occupy today.

9 What should be rights and responsibilities of other entities, such as authorities, or interested third-parties such as civil society organisations or equality bodies in contributing to tackle illegal activities online? 5000 character(s) maximum

Authorities should be empowered and sufficiently resourced to fulfil their respective mission.

For example, law enforcement authorities need to be well staffed and trained to find, properly document, and where appropriate prosecute illegal online activity without violating the fundamental rights of people unrelated to the content, like the right to privacy.

Oversight authorities (EDRi is advocating for strong DSA oversight) should be empowered and sufficiently resourced to police platform operators and enforce the obligations under the DSA. They should also be allowed and empowered to verify the functioning and legality of content moderation algorithms, the way platforms deal with content-related complaints, and the processes in place to do so in respect of people's fundamental rights.

Civil society: While CS can play an important role in creating public awareness and pressure on all stakeholders involved, in defending user rights, and sometimes even in supporting platform operator in making the right choices in terms of content moderation policies. CS should not, however, be employed by the law as a replacement for the responsibilities of platforms or oversight authorities. The law must be enforced by the authorities, not by small non-profits struggling to scrape together funding to go to court against some of the largest and most powerful corporations in the world.

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

Online platforms are free to employ measures, both human-operated and automatic, to find content and activities they believe are incompatible with their terms of service. The DSA should prescribe that such activities and the terms of service governing them must always be appropriate, proportionate, and transparent to users. Users need to be able to understand in clear language under which rules a given platform operates, how to abide by those rules, and what happens if the users break them.

Large online platforms should also put tools in place that empower their users to protect themselves against unwanted legal content. For that aim:

- Users should have a right to have/use fine-grained control over what they see – that control should override any business interest a platform may have in distributing certain content. This includes a right for users to switch off personalised/micro-targeted content (like recommender systems) as well as advertising and algorithmically-curated content

recommendations. Users also need to be fully and transparently informed as soon as they are subjected to such curation and recommendation tools.

- Dominant platforms as defined in EDRi's DSA position paper "Platform Regulation Done Right" should be obliged to allow users from competing platforms with similar functionality to interconnect with friends on the dominant platform. This means, for example, that a dominant messaging platform should allow competing messaging services to enable their users to send messages directly to Facebook Messenger and WhatsApp users, without the need to create a separate account there (service interoperability). This measure—either implemented as a mandatory, public API or as an open, standardised protocol like—would help to considerably reduce network effects that are preventing effective competition in the platform markets on aspects like best content moderation, user control, or privacy protection.

11 In particular, are there specific measures you would find appropriate and proportionate for online platforms to take in relation to potentially harmful activities or content concerning minors? Please explain. 5000 character(s) maximum

See the above, plus platforms should be clear and transparent about whether they are made and safe for minors to use.

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

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

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

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

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

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

3 Adapted risk assessments and mitigation strategies undertaken by online platforms

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

5 Auditing systems over platforms' actions and risk assessments

5 Regulatory oversight and auditing competence over platforms' actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on manipulation and amplification of disinformation.

13 Other, please specify:

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

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

International human rights law puts very strict requirements for the conditions under which states can restrict freedom of expression and information (such as the principles of legality, necessity and proportionality, legitimacy). According to Article 15 of the European Convention of Human Rights, in emergency situations, states can derogate from their obligation in relation to freedom of expression and information but must justify such derogation by meeting two essential conditions: (1) The situation must amount to a public emergency that threatens the life of the nation or war; and (2) the state must have officially proclaimed that state of emergency and notified other countries through the Secretary General of the Council of Europe. In addition, every measure must be strictly required by the exigencies of the situation.

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

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

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

5 Maintaining an effective complaint and redress mechanism

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

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

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

16 Other. Please specify

Beyond content moderation and transparency best practices, platforms should give their users fine-grained control over what they see – that control should override any business interest a platform may have in distributing certain content. This includes a right for users to switch off personalised/micro-targeted content and advertising.

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

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

In order to avoid such fundamental rights violations when regulating online platforms, the first cornerstone consists of measures designed to break open the centralised platform economy that is so conducive to the dissemination of toxic online behaviour. Much of the damage inflicted by content that can cause harm relates to its viral spread and amplification on and by social media platforms. At the moment, users have no choice but to submit themselves to the failing content moderation rules that platform monopolies like Facebook, Twitter or YouTube have tried to establish for over a quarter of the world's population. The DSA has the chance to leave this technological dead-end behind by, among other improvements, requiring dominant social media platforms to open up to competitors with mandatory interoperability. This would allow users to freely choose which social media community they would like to be part of – for example depending on their content moderation preferences and their need for more solid privacy protection – while still being able to connect with and talk to all of their social media friends and contacts.

The second cornerstone is protecting an updated legal liability regime for hosting intermediaries with regard to user-generated content. Any attempt to weaken the current legal liability regime while pushing intermediaries to "take more responsibility" for online expression inevitably leads to the systematic over-removal of legitimate speech by commercial Big Tech companies. Privatising the legality assessment for online expression cannot be the solution. Instead, the EU should improve access to the justice system as proposed in this paper.

The third cornerstone is a workable notice-and-action system that empowers people to notify intermediaries of potentially illegal online content and behaviour they are hosting. While those user notifications should not make intermediaries legally liable for a legality assessment they may make (see second cornerstone), it should oblige them to verify the notified content and reply to the notifier and – where appropriate – the content uploader, with a reasoned decision. The reply should always include clear information about the possibilities for legal redress as well as the reasoning behind an action taken by the intermediary regarding the specific piece of content.

Effective legal redress constitutes the fourth cornerstone for addressing the challenge of illegal online content and behaviour. Content removal is often an inappropriate deterrent for people who post or spread illegal online content. Judicial proceedings can be an appropriate deterrent. In reality, however, regular courts in most EU countries are overwhelmed with content moderation cases from big social media platforms. That is why EDRi proposes the creation of specialised tribunals or independent dispute settlement bodies in EU Member States that are cheaper, faster, and more accessible for affected users to settle speech-related disputes with other users or with hosting

intermediaries. These fully independent tribunals should be financed by dominant commercial intermediaries that are active on the EU market, for example via a 'European Online Content Dispute Settlement Fund' managed at EU level.

No one single solution will protect all fundamental rights in today's centralised platform economy but a combination of smart regulatory measures, as proposed in EDRi's DSA position paper "Platform Regulation Done Right", can help minimise the negative societal effects created by the toxic dissemination and amplification of illegal online content, while protecting the fundamental rights enshrined in the EU treaties.

Questions 18.-19.: no EDRi response

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

Minimum transparency requirements should (1) empower users and return to them the agency and control over information they view on online platforms (2) enable public oversight authorities to fulfil their monitoring function over content recommendation systems in order to ensure the systems' compliance with the protection of fundamental rights.

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

- Users are able to access their full profiling data (including information about and deduced from their online behaviour) in a comprehensible format, including data about and inferred from their behaviour and generated by the platform's algorithms. Existing data protection rules should be complemented with the DSA by addressing the current lack of accessibility and readability of such data. Such behavioural and inferred data fall under the GDPR and therefore data subjects must be able to have this rectified or deleted if they so wish.
- Users are always informed when they are being subjected to algorithmic recommender systems. Explanations of the algorithmic recommender systems should always be accessible and presented to users in tangible and comprehensible language, including information about the family of models, input data, performance metrics and how the model was tested. Such an explanation will allow users to contest the algorithmic decision-making and/or to opt out of it.
- Users always have the right to opt out/switch off the use of such recommender systems, for example on video sharing platforms: which video to watch next; or on marketplaces: which product to buy. In particular, the DSA should guarantee that users' default settings are set as "opt-out" and require them to proactively opt in to personalised content recommendation systems. Platforms should design consent and privacy policies in a way that facilitates informed users' choice.

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

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

Questions 21.: no EDRi response

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

Not in the way this question is phrased, as it is unclear what "enhanced data sharing" means. Does this mean "more data sharing" in terms of frequency, or with less checks and balances? Of course platforms can always voluntarily share data within the boundaries of the GDPR.

Law enforcement authorities and the judiciary already have ample rights to request data from platform operators as part of judicial investigations and proceedings, and thanks to the European Investigation Order this also works across borders. The DSA should not give law enforcement additional powers to access data.

Whether areas like labour rules, tax law and social security regulations should be included in the DSA (legal basis?) is certainly unclear, too.

23 What types of sanctions would be effective, dissuasive and proportionate for online platforms which systematically fail to comply with their obligations (See also the last module of the consultation)? 5000 character(s) maximum

Financial sanctions should follow the example set by the GDPR and also include behavioural remedies such as interoperability, transparency, and internal procedural requirements.

Questions 24.: no EDRi response

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, to 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 the 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 the functioning of the current liability exemption regime and the areas where an update might be necessary.

Questions 1.: no EDRi response

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

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

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

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

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

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

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

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

or be held legally liable for it. This does not preclude platforms' responsibility for their own actions such as the promotion, demotion, or micro-targeting of user-generated content.

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

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

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

4 Does the current legal framework disincentivize 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

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

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

5 Do you think that the concept characterising intermediary service providers as playing a role of a 'mere technical, automatic and passive nature' in the transmission of information (recital 42 of the E-Commerce Directive) is sufficiently clear and still valid? Please explain. 5000 character(s) maximum

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

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

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

should not lead to the loss of liability exemption under Article 14 of the E-Commerce Directive. The Advocate General's reasoning is just as true for the DSA: "Otherwise, there would be a risk of platform operators becoming judges of online legality and a risk of 'over-removal' of content stored

by them at the request of users of their platforms in so far as they also remove legal content." (source: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200096en.pdf).

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

6. The E-commerce Directive also prohibits Member States from imposing on intermediary service providers general monitoring obligations or obligations to seek facts or circumstances of illegal activities conducted on their service by their users. In your view, is this approach, balancing risks to different rights and policy objectives, still appropriate today? Is there further clarity needed as to the parameters for 'general monitoring obligations'? Please explain. 5000 character(s) maximum

Yes, the prohibition of any general monitoring obligation is one of the cornerstones of a successful internet regulation. General monitoring consists of the indiscriminate verification and control of all the online content or behaviour hosted on intermediaries' systems for an unlimited amount of time and thus requires the mandatory use of technical filtering tools against all users. Such an obligation would have inevitable detrimental effects on the ability of people who have done nothing wrong to freely share and access content online. Requiring intermediaries to actively look for potentially illegal content with the aim of removal also implies that platform operators should have the ability and incentive to properly assess whether any given piece of content is actually illegal under EU law or any of the 27 member state laws. Practice and common sense shows that they have neither and would be pretty bad replacements for our ordinary and criminal courts.

7. Do you see any other points where an upgrade may be needed for the liability regime of digital services acting as intermediaries? 5000 character(s) maximum

No.

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

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

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/ No reply
Consumers have sufficient choices and alternatives to the offerings of online platforms.					X	
It is easy for consumers to switch between services provided by online platform companies and use same or similar services provider by other online platform companies					X	

("multi-home").						
It is easy for individuals to port their data in an useful form for alternative service providers outside of an online platform.					X	
There is sufficient level of interoperability between services of different online platform companies.					X	
There is an asymmetry of information between the knowledge of online platforms about consumers, which enables them to target them with commercial offers, and the knowledge of consumers about market conditions.	X					
It is easy for innovative SME online platforms to expand or enter the market.					X	
Traditional businesses are increasingly dependent on a limited number of very large online platforms.	X					
There are imbalances in the bargaining power between these online platforms and their business users.	X					
Businesses and consumers interacting with these online platforms are often asked to accept unfavourable conditions and clauses in the terms of use/contract with the online platforms.	X					
Certain large online platform companies create barriers to entry and expansion in the Single Market (gatekeepers).	X					
Large online platforms often leverage their assets from their primary activities (customer base, data, technological solutions, skills, financial capital) to expand into other activities.	X					
When large online platform companies expand into such new activities, this often poses a risk of reducing innovation and deterring competition from smaller innovative market operators.	X					

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

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

	1	2	3	4	5
Large user base					X
Wide geographic coverage in the EU				X	
They capture a large share of total revenue of the market you are active/of a sector		X			
Impact on a certain sector				X	
They build on and exploit strong network effects					X
They leverage their assets for entering new areas of activity			X		
They raise barriers to entry for competitors					X
They accumulate valuable and diverse data and information					X
There are very few, if any, alternative services available on the market				X	
Lock-in of users/consumers					X
Other					

2. If you replied "other", please list

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

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

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

X search engines

X operating systems for smart devices

X consumer reviews on large online platforms

network and/or data infrastructure/cloud services

X digital identity services

X payment services (or other financial services)

physical logistics such as product fulfilment services

data management platforms

X online advertising intermediation services

Other. Please specify in the text box below.

5 Other - please list 1000 character(s) maximum

All types of operating systems (not only for "smart devices") can be used by an operator as a tool to abuse its gatekeeper role. Providing the basis for all other software running on a device, the OS usually controls aspects such as:

- What kind of access users have to basic device functionality: this gives OS makers the power to limit extending a devices functionality through third-party products;
- What kind of software/apps are allowed to run on the device: this gives OS makers the power to prevent users from installing software or apps offered by competitors or providers of services that the gatekeeper plans to enter;
- The user's personal data: the OS usually has access to all parts of the memory and storage and therefore to all personal data that other apps store on the device. In addition, OS makers can collect comprehensive usage/behavioural data across all other software/apps used on that device.

Emerging issues

Questions 2.-7.: no EDRi response

The following questions are open to all respondents.

9. Are there specific issues and unfair practices you perceive on large online platform companies? 5000 character(s) maximum

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

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

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

4. Facebook makes it impossible for competing social networks to enable their users to interconnect with friends on Facebook. Thereby, the company abuses its market power and strong network effects to lock-in its users, to artificially prevent them from getting in touch with 'the

outside world', and to suppress any potential competing social network from ever gaining a foothold in that market—most users are already taken by Facebook.

10 In your view, what practices related to the use and sharing of data in the platforms' environment are raising particular challenges? 5000 character(s) maximum

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

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

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

Furthermore, the DSA could prohibit advertisers to target users with content based on very sensitive personal data, such as their specific psychological profiles, political opinions, sexual orientations, health status, or any other sensitive personal data. This limitation should include all types of content, no matter if it is political, issue-based, commercial, or otherwise. This would not impede the use of online advertising: publishers, bloggers, app developers, and others can still use generic or context-sensitive online ads in order to generate revenue without collecting any personal data about users.

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

- In how many cases were contested removals reversed?

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

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

11 What impact would the identified unfair practices can have on innovation, competition and consumer choice in the single market? 3000 character(s) maximum

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

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

Example 3: Facebook's combining of personal data without user choice has an immense negative impact on consumer privacy rights. The more companies and digital services that Facebook buys and operates, the harder it will be for people to use services without being forced to give up their personal data to Facebook. The situation is aggravated by the inclusion of Facebook tracking code into many major websites (such as the "Like" button). This code channels personal data to Facebook

whenever someone visits a website, regardless of whether that person has a Facebook account or not.

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

Questions 12.: no EDRi response

13 Which are possible positive and negative societal (e.g. on freedom of expression, consumer protection, media plurality) and economic (e.g. on market contestability, innovation) effects, if any, of the gatekeeper role that large online platform companies exercise over whole platform ecosystem? 3000 character(s) maximum

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

- By reducing the diversity of online platforms, the gatekeeper prevents fair competition on how to best deal with illegal content or how to best protect users against harm. As a result, it is not only users but also regulators and legislators who depend on one single private company to come up with viable solutions rather than being able to choose from the best ideas in the market. In a gatekeeper scenario, regulators and legislators also have no choice but to trust the gatekeeper when they claim there are no better solutions than theirs.
- For social networks, the gatekeeper role centralises an immense power over what people see and read, and what publishers can successfully distribute online. A social network's content curation algorithm can decide how many readers a journalistic work will reach and which leaked documents are being censored (see the example of #BlueLeaks suppressed by Twitter). Usually those algorithms are neither transparent nor verifiable. Add to this, that advertising-funded companies like Youtube or Facebook don't even attempt to provide fair or balanced content curation; instead they promote and demote content depending on what makes people stick to their screens: scandal, outrage, hate, social division. This unhealthy dependence on a single, centrally-controlled 'information bottleneck' is at least partly responsible for the difficult situation press publishers are in today.
- Gatekeepers often also stifle innovation and prevent the success of new entrants. For example, Facebook acts as gatekeeper to 2.5+ billion social network users. Multi-homing in social networks does not seem to be possible, so the only way to reach those users with

similar functionality would be to be interoperable with Facebook. But that's something the company actively prevents to protect their gatekeeper role. The same can be said of Apple, which—by prohibiting alternative software sources on iOS devices—uses its gatekeeper position as the only operating system provider for Apple devices to prevent competing app stores (and thereby potentially competing apps) to enter the market on iOS app stores.

Question 14.: no EDRi response

Regulation of large online platform companies acting as gatekeepers

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

» I fully agree

I agree to a certain extent

I disagree to a certain extent I disagree

I don't know

2 Please explain 3000 character(s) maximum

The DSA should put in place rules, such as mandatory interoperability, that are able to limit the gatekeeper role that large online platform companies have acquired, as well as the resulting negative effects. Such rules need to be specific to these gatekeepers as they would otherwise risk hurting smaller players trying to compete with them. As a result, the goal of increased user choice and freedom would not be achieved. Interoperability mandates would also breathe life into the data portability right introduced by the GDPR that has been of little use so far because of a lack of spaces where users could port their data to. Currently, it is unclear what personal data users are able to port and under which circumstances. Thus, the DSA should also clarify the GDPR's data portability right.

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

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

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

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

» Yes

No

I don't know

4 Please explain your reply and, if possible, detail the types of **prohibitions** that should in your view be part of the regulatory toolbox. 3000 character(s) maximum

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

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

» Yes

No

I don't know

6 Please explain your reply and, if possible, detail the types of **obligations** that should in your view be part of the regulatory toolbox. 3000 character(s) maximum

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

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

» Yes

No

I don't know

8 Please explain your reply. 3000 character(s) maximum

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

An independent European regulatory authority should therefore be tasked to oversee compliance with these obligations. The regulator should be tasked with monitoring and enforcing compliance, issuing fines, auditing intermediaries covered by the DSA, as well as receiving complaints from affected individuals and organisations. It must be equipped with enough resources to effectively control and enforce the obligations for gatekeepers and all other entities covered by the DSA and should have proven experience in the field of internet regulation, the platform economy and fundamental rights.

The independent regulator should not, however, be empowered to take content moderation or content decisions, as such decisions should ultimately be in the hands of the independent judiciary.

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

» Yes

No

I don't know

10 If yes, please explain your reply and, if possible, detail the types of case by case remedies. 3000 character(s) maximum

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

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

» Yes

No

12 Please explain your reply 3000 character(s) maximum

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

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

the same regulatory authority or could they be enforced by different regulatory authorities? Please explain your reply. 3000 character(s) maximum

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

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

At national level

» At EU level

Both at EU and national level.

I don't know

Question 15.: no EDRi response

16 Should such rules have an objective to tackle both negative societal and negative economic effects deriving from the gatekeeper role of these very large online platforms? Please explain your reply. 3000 character(s) maximum

Yes, both perspectives can be taken into consideration. In this case, the DSA must however clearly specify the objectives that a regulator is allowed to pursue. Concretely, the regulator should not be able to impose remedies on a gatekeeper vaguely citing some "negative societal effects". The DSA should include a concrete list of such effects that would empower the regulator to act. This is crucial for protecting legal certainty for companies and for limiting the powers of the regulator to what is necessary and appropriate.

17 Specifically, what could be effective measures related to data held by very large online platform companies with a gatekeeper role beyond those laid down in the General Data Protection Regulation in order to promote competition and innovation as well as a high standard of personal data protection and consumer welfare? 3000 character(s) maximum

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

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

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

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

Questions 18.: no EDRi response

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

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

» Pan-EU scope

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

» Capacity building within Member States

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

Cooperation with extra-EU jurisdictions

» Other

20 If other, please specify 3000 character(s) maximum

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

Questions 21.: no EDRi response

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

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

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

» Investigative powers for the public authority

» Other

23 Other – please list 3000 character(s) maximum

Powers for the regulator to investigate the use of algorithms for content curation and moderation, to investigate the use of personalised/micro-targeted advertisement systems, and to investigate claims for breaches of obligations under the DSA.

Questions 24.: no EDRi response

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

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

4 There is a need for an additional regulatory framework imposing obligations and prohibitions that are generally applicable to all large online platforms with gatekeeper power

4 There is a need for an additional regulatory framework allowing for the possibility to impose tailored remedies on individual large online platforms with gatekeeper power, on a case- by-case basis

5 There is a need for a New Competition Tool allowing to address structural risks and lack of competition in (digital) markets on a case-by- case basis.

5 There is a need for combination of two or more of the options 2 to 4.

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

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

Questions 27.: no EDRi response

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

Online advertising

1 When you see an online ad, is it clear to you who has placed the advertisement online?

Yes, always

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

» **Sometimes: but I cannot always find this information**

I don't know

No

Questions 2.-14.: no EDRi response

15 From your perspective, what measures would lead to meaningful transparency in the ad placement process? 3000 character(s) maximum

EDRi calls for the implementation of strong privacy and data protection rules, transparency and a legally binding, human-rights based approach. Paired with meaningful enforcement, this will ensure that the online advertising industry can be held accountable for the way it shapes our online environment. Regarding ad placement, understanding the way in which Real Time Bidding (RTB) works and how ads are allocated is essential for policy-making regarding this type of platform.

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

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

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

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

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

Finally, the promotion of tracking-free ad business models (like the one at NPO: https://brave.com/npo) and further research are essential steps in the right direction. Similar actions to protect readers' privacy have been launched by the New York Times (see https://open.nytimes.com/how-the-new-york-times-thinks-about-your-privacy-bc07d2171531?gi=31439d22e80c).

16 What information about ads displayed online should be made publicly available 3000 character(s) maximum

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

According to EDRi member Privacy International, this information should include at least: 1) the source of the data used to target ads, 2) the target audience of the advertiser and actual audience of the advertiser, 3) information about if the ad was micro-targeted (see https://www.privacyinternational.org/explainer/3288/why-advertising-transparency-important).

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

Mandatory ad libraries should at least include:

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

17 Based on your expertise, which effective and proportionate auditing systems could bring meaningful accountability in the ad placement system? 3000 character(s) maximum

Any auditing system must include an obligation for platforms to produce thorough documentation of their algorithms used for ad targeting, including fairness criteria for their ad optimisation process, in particular the obligation to conduct and publish Human Rights Impact Assessments. For details

about such Impact Assessments and auditing mechanisms please see EDRi member Panoptykon's AI position paper: https://panoptykon.org/sites/default/files/stanowiska/panoptykon_ai_whitepaper_submission_10.06.2010_final.pdf.

18 What is, from your perspective, a functional definition of 'political advertising'? Are you aware of any specific obligations attaching to 'political advertising' at a European or national level ? 3000 character(s) maximum

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

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

Question 19.: no EDRi response

20 What impact would have, in your view, enhanced transparency and accountability in the online advertising value chain, on the gatekeeper power of major online platforms and other potential consequences such as media pluralism? 3000 character(s) maximum

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

For example public broadcasters such as NPO (see https://brave.com/npo) are already providing very successful alternatives to the current invasive business models which can be applied to most of the other public and private publishers and broadcasters. Through this change, NPO have been able to even increase (see https://www.openrightsgroup.org/blog/is-ethical-ad-tech-possible) their

advertising profits after deciding not to track the people accessing their services, even during the COVID pandemic where most advertising revenues were going down.

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

21 Are there other emerging issues in the space of online advertising you would like to flag? 3000 character(s) maximum

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

https://algorithmwatch.org/en/story/left-on-read-facebook-data-access); and (b) more details on recommendations linked to political advertising, see https://panoptykon.org/political-ads-report.

- Recommendation and content moderation algorithms must be audited (see https://arxiv.org/pdf/2001.10581.pdf). Online advertising companies and platforms using their services for advertising purposes should be transparent about the use and any practical impact of the automated tools they use.

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

The following questions are targeted at all respondents.

Governance of digital services and aspects of enforcement

Question 1.: no EDRi response

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

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

5 Cooperation mechanism within Member States across different competent authorities responsible for the systematic supervision of online platforms and sectorial issues (e.g. consumer protection, market surveillance, data protection, media regulators, anti-discrimination agencies, equality bodies, law enforcement authorities etc.)

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

4 Coordination and technical assistance at EU level

5 An EU-level authority

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

5 Other: please specify in the text box below

3 Please explain 5000 character(s) maximum

Any regulatory/oversight body must be equipped with sufficient resources including financial and human, in order to be able to fulfil its mandate. The rag rug of poorly financed, understaffed data protection authorities in member states created by GDPR has shown that failing to enforce an otherwise well-done legislation can render crucial regulation toothless.

Cooperation schemes with civil society and academics can be useful but should not lead to an outsourcing of regulatory or oversight responsibility to non-governmental actors. The law must be enforced by the authorities, not by small non-profits struggling to scrape together funding to go to court against some of the largest and most powerful corporations in the world.

4 What information should competent authorities make publicly available about their supervisory and enforcement activity? 3000 character(s) maximum

At a minimum, competent authorities should publish:

- All their enforcement decisions such as decisions for remedies or sanctions/fines, including a comprehensive reasoning;
- Explanatory notes summarising each investigation for non-expert readers;

- All raw data and supporting documents that were collected or analysed as part of investigations. These data and documents should be redacted to a minimum and only to protect the respective company's IP and personal data.

5 What capabilities – type of internal expertise, resources etc. - are needed within competent authorities, in order to effectively supervise online platforms? 3000 character(s) maximum

Employees of competent authorities should have proven experience in the field of internet regulation, the platform economy and fundamental rights. They should never have any conflicts of interest with the companies they oversee. This is particularly necessary as big tech firms systemically co-opt or co-finance the work of academics and other experts through grants—something that can potentially affect a person's independence.

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

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

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

No

Other

I don't know

Question 7.: no EDRi response

8 How should the supervision of services established outside of the EU be set up in an efficient and coherent manner, in your view? 3000 character(s) maximum

An EU regulator would have the ability to oversee service providers established outside of the EU regardless of their official company seat.

Questions 9.-14.: no EDRi response