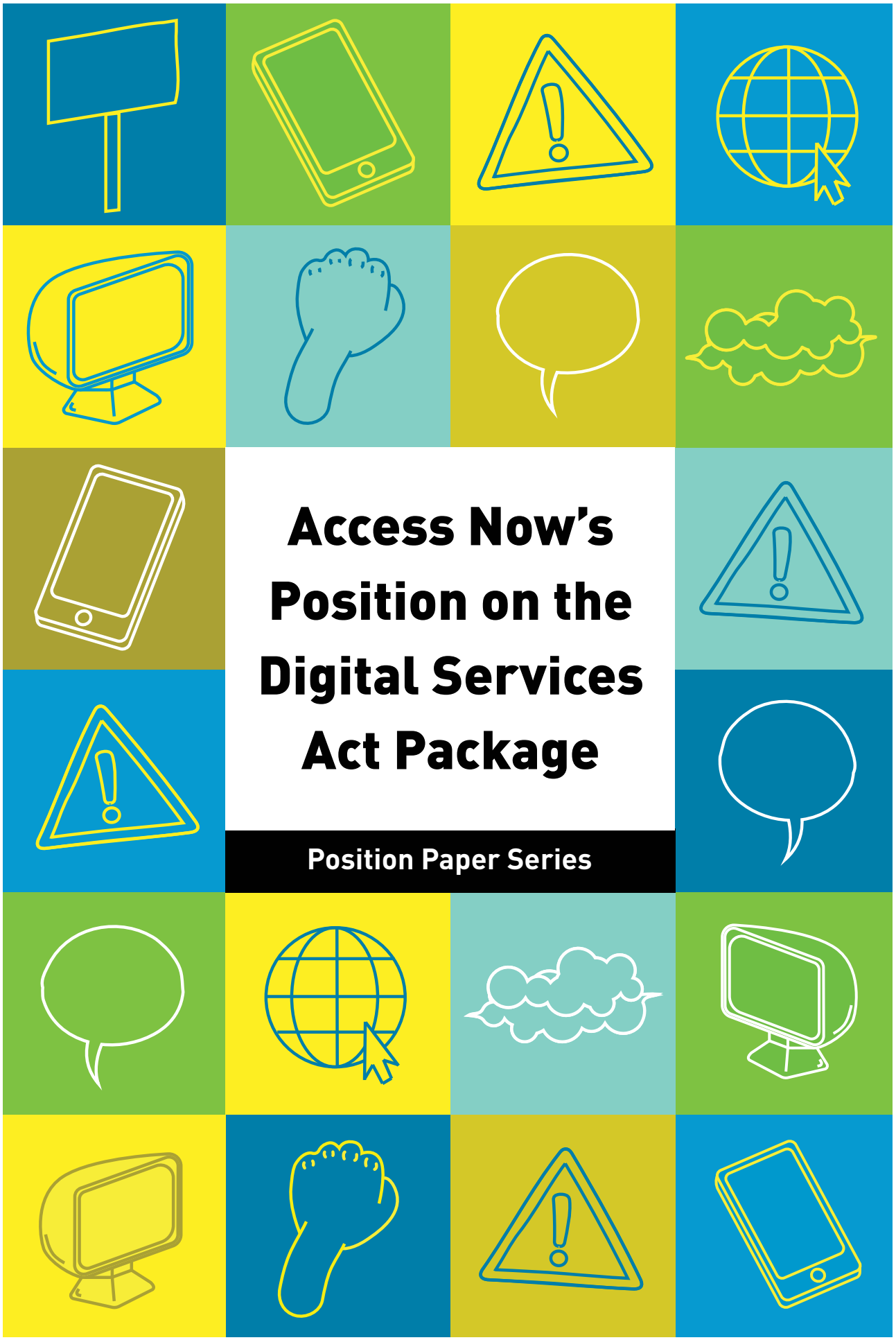


Access Now's Position on the Digital Services Act Package

Position Paper Series

accessnow

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

Access Now's Position on the Digital Services Act Package

POSITION PAPER SERIES | SEPTEMBER 2020

SUMMARY

This set of three position papers presents Access Now's position on the upcoming Digital Services Act (DSA) legislative package. The series addresses the issues we have identified as priorities in our policy and advocacy work, comprising

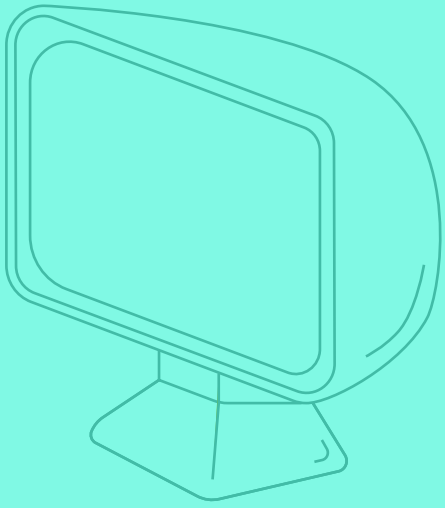
1. **A human rights-based legal framework for intermediary liability;**
2. **A human rights response to the amplification of potentially harmful legal user-generated content; and**
3. **A proposal for the effective oversight and enforcement mechanism of the DSA legislative framework.**

Each paper has a set of policy recommendations that are informed by our global expertise in content governance, data protection, the protection of users' privacy, and the human rights implications of artificial intelligence.

For more information:
Eliška Pírková (eliska@accessnow.org)

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

1. Human Rights-based Framework for Intermediary Liability in Europe



1. Human Rights-based Framework for Intermediary Liability in Europe

POSITION PAPER | SEPTEMBER 2020

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 2
II. PROBLEM DEFINITION 2
III. DEFINED SCOPE 3
IV. DEFINED PROCEDURES 3
V. TRANSPARENCY 6
VI. PROCEDURAL FAIRNESS 6
VII. ACCESS TO ADEQUATE REMEDY 6
VIII. POLICY RECOMMENDATION 7
Foreseeable legal framework to regulate gatekeepers 7
Adequate response mechanisms 8
Due process safeguards 10
IX. CONCLUSION 12

I. EXECUTIVE SUMMARY

Since 2010, the European Union (EU) has issued several regulatory and co-regulatory efforts to combat illegal content online under the umbrella of the Digital Single Market initiatives. All of these efforts have one common element: to shift more responsibility for combatting illegal content onto large online platforms that have gained the position of gatekeepers of fundamental rights. The most worrisome aspect of these regulatory efforts is the fact that the European Commission delegated the development of human rights and due diligence safeguards for users' fundamental rights to private companies. This way, gatekeepers have been replacing the role of the state, often acting as quasi-judicial bodies and exercising privatised law enforcement in online spaces. Such an approach significantly weakens the human rights protection of online users as well as legal certainty for all parties involved. However, there is a chance to reverse this logic with the upcoming legal review of the e-Commerce Directive that will be upgraded by a new set of rules under the Digital Service Act (DSA) legislative package. There is a strong need to establish a harmonised and coherent approach to content governance across the EU, which is currently missing. The European Commission has an extraordinary chance to stop "offloading" state obligations on private companies and to develop the rules these actors should follow, especially gatekeepers whose role in democratic societies has become irreplaceable.

We provide an overview of our recommendations and digital rights safeguards, which we explore in detail in Section VIII. They fall under three pillars.

The three main areas of our recommendations are:

1. **Adopt a foreseeable legal framework to regulate gatekeepers of fundamental rights**
2. **Develop adequate response mechanisms to illegal user-generated content**
3. **Adopt and enforce due process safeguards that are easily accessible and available to online users**

NOTE TO READERS

Please direct your queries or comments to the following Access Now policy team members:
Eliška Pírková (eliska@accessnow.org)

II. PROBLEM DEFINITION

There are multiple issues with the existing intermediary liability regime in the EU. The prevailing policy incoherence at the EU level and large disparities among Member States in implementing the e-Commerce Directive have a negative impact on the fundamental rights of online users. Experts have been underlining for years how the current intermediary liability regime leads to over removal of legitimate speech. The lack of legal certainty has given online platforms the incentive to develop and enforce disproportionate responses to potentially illegal content.

This position paper provides the main fundamental rights safeguards that should be enshrined in the upcoming DSA legal framework, while reflecting on current vulnerabilities and regulatory gaps.

III. DEFINED SCOPE

Gatekeepers of information society

The European Commission has to take into consideration the specific features of online platforms, such as their size, functionality, and the type of services they offer. Systemic platforms that play the role of gatekeepers of information society should have greater responsibility than actors that have a smaller impact in the Digital Single Market. The gradual scaling of responsibility, based on a platform's market share and other forms of dominance, should be determined using criteria to assess their market power and their position to shape and influence public discourse. In other words, the greater a platform's cost to individuals' fundamental rights and the capacity of smaller private actors to compete, the greater the need for regulation that will protect users' best interests. Based on this reasoning, nonprofit organisations should benefit from a comparatively less restrictive liability regime than platforms that curate and moderate online content for profit.

Categories of user-generated content and activity: illegal vs "harmful" content

The DSA legislative package should only tackle illegal content online. "Harmful" content should be left outside the DSA's scope, as the concept of harm is inherently vague and including it may lead to human rights abuses. Furthermore, the concept of "legal but harmful" content represents a serious challenge to the legality principle. However, the future legislative framework can and should establish a set of minimum transparency and accountability requirements for online platforms, especially those enforcing their Terms of Service (ToS). The European Commission should make sure that content moderation and distribution tools are sufficiently transparent and that online users always have easy access to effective remedy and redress mechanisms.

IV. DEFINED PROCEDURES

"Good Samaritan" like safeguards

In order to safeguard the principle of legal certainty and consequently to prevent the over-removal of legal content by online platforms, the DSA package should establish safeguards similar in concept to the "Good Samaritan"clause. Such safeguards will ensure that online platforms will not be held liable even if they edit, filter, or remove a piece of content that is actually legal. The current European framework lacks such a safeguard for platforms that seek to address illegal and potentially harmful content more proactively, even if they are often pushed by policy makers and state actors to do so via soft law co-regulatory measures. Such lack of legal certainty incentivises over-removals and over-compliance with policy initiatives in order to escape legal liability.

Tailored Notice-and-Action procedures

The European Commission should not underestimate the importance of a legislative framework specifying details of Notice-and-Action (N/A) procedures because it significantly improves foreseeability and legal certainty for all regulated parties. The DSA legislative package should establish N/A procedures for online platforms that curate and moderate user-generated content. Different types of illegal online content and activities require different responses specifically tailored to the type of user-generated content in question. However, the legislative framework has to clearly define the procedures and provide appropriate safeguards for their application. Access Now recommends a scaled model of responsibility for online platforms and adoption of adequate N/A procedures that are tailored to specific categories of user-generated content. As an example of a good practice, we recommend the following models of N/A procedures:

- **Notice-and-judicial takedown** should be required for illegal user-generated content. Under this mechanism the content can be removed only on the basis of a judicial order. If an online platform fails to comply with a judicial order, it will be held liable. Law enforcement authorities should be able to issue the notice but only under conditions strictly defined by the legislative framework. However, such a notice has to be backed up by a judicial order. In other words, the assessment of the legality of a piece of content needs to be performed by an independent judicial authority. In cases when a piece of content that is manifestly illegal content irrespective of its context, such as content involving child sexual abuse material,[1] directly endangers an individual's physical integrity and wellbeing, law enforcement should be able to issue an order with direct suspensive effect. This emergency measure will ensure that the law enforcement authority will have to submit its removal order to the platform, and at the same time, to an independent judicial authority that will conduct judicial review of the presumed illegality. The content in question would be restricted temporarily for the concrete time frame prescribed by law. The interference could not be prolonged beyond this allocated time frame. During this time, the judicial authority would conduct the judicial review of the order and consequently notify law enforcement as well as the platform of its final decision. When an independent judicial authority does not confirm the legality of a removal order issued by law enforcement, the restoration of illegitimately restricted content has to be secured swiftly and the content provider has to be notified of the outcome, accompanied with adequate reasoning.

- **Notice-and-notice mechanisms** have proven to provide the most balanced measure for tackling copyright infringements. For instance, Canada's notice-and-notice model for copyright law is an innovative model that moves away from a liability framework and rather focuses on **action requirements for intermediaries** that serve an educational function for users. Based on this model, a **Notice-and-notice plus mechanism** could be made applicable in cases of defamation, as proposed by Emily Laidlaw and Hilary Young to the Law Commission of Ontario.[2] Once a platform receives a notice, whether from a private party or trusted flaggers, it forwards the notice to a content creator within a prescribed

[1] Manifest illegality of user-generated content should always be determined by an independent judicial authority, as suggested by the Council of Europe, Recommendation CM/Rec(2018)2of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries.
[2] Emily Laidlaw, Hilary Young (2017). Internet Intermediary Liability in Defamation: Proposal for Statutory Reform. Retreived from http://www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-Laidlaw-and-Young.pdf

time frame. The content creator is given a chance to submit a counter-notice within a specified time frame prescribed by law and which then has to be delivered by the platform to the complainant in a reasonable time. If the content creator responds to the notice of a complaint, the online platform is not required to take any further steps and the content remains in circulation. It is then up to the complainant to obtain a judicial order for content removal. On the other hand, if a content creator fails to respond to a notice within a prescribed time frame, the platform disables the access to the disputed content. Under such a model, if an online platform fails to comply with these rules, it should be subjected to financial sanctions rather than being stripped of its liability exemption. Several aspects of this model should be codified by the legislative framework. These include specifying the required information that such a notice needs to contain in order to be valid; the requirement of a declaration of good faith submitted by complainants as a safeguard against abusive notices; and the requirement that no general monitoring obligation be imposed on platforms. Online platforms should not be required to provide the personal information and identity of a content creator, if the content was posted anonymously or under a pseudonym.

No general monitoring

The DSA legislative package should uphold the prohibition of general monitoring as stipulated by Article 15 of the e-Commerce Directive. This type of monitoring violates the rights to freedom of expression and privacy and therefore should never be imposed on online platforms. Similarly, the Council of Europe Recommendation on the roles and responsibilities of internet intermediaries establishes that state authorities "should not directly or indirectly impose a general obligation on platforms to monitor content which they merely give access to, or which they transmit or store, be it by automated means or not."[3] In his 2018 report on the promotion and protection of the right to freedom of opinion and expression, the UN Special Rapporteur David Kaye clarifies that states should refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content, as it would be both inconsistent with the right to privacy and likely to amount to pre-publication censorship.[4]

Obtaining actual knowledge

In order to strengthen legal certainty for online platforms, the DSA legislative package should establish when and how online platforms obtain actual knowledge of illegal content on their services. It should clearly state what online platforms need to know in order to trigger the obligation to remove illegal content. Online platforms should not act as quasi-judicial bodies or be required to assess the legality of user-generated content.

Valid notice

The DSA package should provide clearly defined minimum criteria of what constitutes a valid notice. Rules specifying the requirement of valid notice are particularly important because the

[3] Council of Europe (2018). Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries.
[4] United Nations General Assembly (2018). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/73/348. Retrieved from https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ReportGA73.aspx

notice determines the existence of actual knowledge, which ultimately determines whether the online platforms can or cannot benefit from the liability exemption.

V. TRANSPARENCY

Transparency is an essential aspect of any legislative framework that seeks to establish human rights safeguards and a user-centric response to illegal content online. The DSA package should ensure that N/A procedures are conducted in a transparent manner. In other words, N/A procedures should be easily accessible, easy to use for all users, clear in their wording, and visible on platforms' websites. This position paper provides recommendations for meaningful transparency that should be reflected in online platforms' transparency reports and directly bound to N/A procedures. Meaningful transparency requirements regarding algorithmic content curation, the application of platforms' ToS, and automated decision-making in content moderation, are covered in the other two position papers in this series on the DSA.

VI. PROCEDURAL FAIRNESS

Notifications to content providers

Notification that is sent to the content provider before any action is taken with regard to the piece of content introduces due process safeguards into the N/A procedures. The purpose of a notification to the content provider is to inform the content provider that a complaint has been made about their content. The extent to which content providers are informed may differ based on the triggered N/A procedure as well as the category of the user-generated content in question. Importantly, notifications to content providers enable them to respond and defend themselves.

Counter-notification

Counter-notification strengthens the right to fair trial for content providers. It enables them to respond to the evidence and observations that were made by a complainant. This way, content providers are able to present their arguments on equal footing. Currently, the counter-notice is enforced by some national legal frameworks of Member States, such as those of Finland or Hungary. We recommend the European Commission assess the best existing practices and base the structure of the regulatory framework establishing N/A procedures on these findings.

VII. ACCESS TO ADEQUATE REMEDY

Defined appeal procedures

Whatever the outcome of N/A procedures is, online platforms should always provide reasoned decisions explaining platforms' actions with regard to the content that was notified. The decision should be delivered to all parties, accompanied by an explanation of the rights of content providers and clearly formulated instructions on how to appeal the decision. The same rule should apply for counter-notices, whether they are rejected or there is a finding in favour of the content

provider. Once the decision is delivered, the appeal procedure has to be made available not only to those users who sought to have the content removed but also to content providers. The appeal procedure at the platform level can provide for remedies, such as rectification, apology, detailed reply, explanation, corrections, or combinations of several forms of remedy in one. However, this form of remedy should not replace effective judicial remedy and judicial redress.

Effective judicial review

Judicial review must always be available to online users. It must be noted that any N/A procedure requires the European Commission to explore new options for easily accessible judicial redress to all online users as well as possible alternative dispute settlements. Judicial redress should always be available to all affected parties, regardless of which N/A procedures were triggered.

VIII. DETAILED POLICY RECOMMENDATIONS

Our key recommendations are based on global expertise in content governance and the protection of freedom of expression online. There are many currently pending legislative efforts to tackle the spread of illegal or potentially harmful content around the world. Besides the upcoming DSA legislative package, Section 230 of the Communications Decency Act in the United States, which is considered the most influential Safe Harbour provision worldwide, is soon to be opened for legal review. Importantly, the European regulatory framework, whether at the EU or Member State level, often has an impact that reaches beyond the EU. Therefore it is essential for the European Commission to strengthen protections for online users as the highest priority.

Adopt a foreseeable legal framework to regulate gatekeepers of users' rights

The legislative framework has to be clear and precise. The European Commission has to ensure that the DSA package applicable to online platforms and to their relations with Member States and users is accessible and foreseeable.

1. Define the scope of the legislative frameworks.	The scope of the DSA package should distinguish between smaller players and large online platforms. Gatekeepers of fundamental rights should hold a larger scale of responsibilities than actors with less impact in the Digital Single Market. The gradual scaling of responsibility based on a platform's market and other forms of dominance should be determined by the set of criteria to assess their market power and their position to shape and influence public discourse. The European Commission should consider the following criteria to determine which platforms fulfill the role of gatekeepers should be considered by the European Commission: ➔ number of users impacted or potentially impacted by a platform's operations; ➔ the platform's yearly economic revenue;

	➔ their position of technical control over users' communications; and ➔ their degree of participation in editing or curation of content, leveraging a vast amount of users' data as well as analysis of behavioural patterns.
2. Ensure that the legislative framework regulates illegal user-generated content only.	The DSA legislative package should regulate only illegal online content. "Harmful" online content should be left outside the DSA scope, as the concept is inherently vague and its use may lead to human rights abuses.
3. Uphold the prohibition of general monitoring.	The DSA package should uphold the prohibition of general monitoring by online platforms. The DSA should not impose an obligation on online platforms to deploy proactive measures to detect illegal content or activities. In order to comply with such an obligation, platforms would apply content-recognition technologies that would ultimately result in general monitoring of all user-generated content hosted by platforms. The European Commission should also refrain from encouraging online platforms to deploy proactive measures on a voluntary basis. While the CJEU jurisprudence allows for so-called specific monitoring of user-generated content, it should not be mandated and specified by the legislative framework.
4. Establish "Good Samaritan" like safeguards.	Voluntary or proactive measures taken by online platforms based on their own initiative should not result in their losing liability exemption.

Develop adequate response mechanisms

The DSA legislative framework should provide a clearly defined procedure for Notice-and-Action mechanism (N/A) as well as exact steps that need to be taken by involved parties.

1. Design adequate response mechanisms tailored to specific categories of user-generated content.	The DSA package should enforce the most appropriate Notice-and-Action mechanisms that are the least intrusive to the policy goal they seek to achieve. Different categories of illegal content will require different responses. The European Commission should provide the evaluation of all restrictions on the right to freedom of expression imposed by adopted measures before and after their application. The full immunity as well as notice-and-stay-down are the most prone to human rights abuse, and therefore should be excluded from the DSA legal framework. When designing adequate N/A mechanisms,

	policy-makers should follow the "fair-balance-as-compromise" principle developed by experts from academia.[5]
2. Establish what constitutes actual knowledge.	In order to safeguard the principle of legal certainty, the DSA should clarify what constitutes actual knowledge about illegal content being hosted by online platforms. The legal framework should provide for minimum standards when this type of knowledge is obtained by platforms. The court order issued by an independent judicial body should always constitute actual knowledge. Platforms' failure to comply with the court order should result in the loss of liability exemption.
3. Provide formal requirements for valid notice.	Formal requirements for valid notice are an essential part of the DSA legislative framework. The information that defines the valid notice sets the whole mechanism in motion. Thus, the valid notice has to be sufficiently precise and adequately substantiated. The basic elements of valid notice should be: ➔ A clearly formulated reason for a complaint accompanied with the legal basis for the assessment of the content; ➔ Exact location of the content that can be determined by the URL link; ➔ Evidence that substiantates the claim submitted by a notifier; ➔ Identity of a notifier only if it is necessary for further investigation of the claim and in full compliance with existing legal standards. In general, notifiers should not be forced to disclose their identity when reporting content. ◆ In case of private disputes, such as copyright infringement and defamation, the identity of the content provider should remain anonymous if the content was posted anonymously or under a pseudonym. ➔ Declaration of good faith in cases of private disputes, such as defamation and copyright infringement.
4. Specify appropriate time frames for N/A procedures.	Notifiers who seek to report the content or challenge unjustified removals by platforms should be able to know the exact steps that need to be taken. Specified time frames and defined procedures should be also followed by intermediaries. The N/A procedure should provide the following information: ➔ the time to forward the notification to the content provider; ➔ the time for the content provider to respond with a counter-notification;

[5] Christina Angelopoulos, Stijn Smets (2016). Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability. Retreived from https://www.ivir.nl/publicaties/download/Notice_and_Fair_Balance.pdf

	➔ the time to make a decision about removing content or maintaining it online; ➔ the time to inform the involved parties about the decision taken; and ➔ the time to initiate a review of the decision by the courts.[6] We urge the European decisionmakers to refrain from imposing short and unreasonable time frames for content removal that will increase the over-removal of legitimate speech from platforms. Time frames such as a one-hour deadline for removal of alleged online terrorist content and 24 hours for removing online hate speech have recently been pronounced unconstitutional by the Constitutional Council of France due to their negative impact on users' right to freedom of expression.
5. Establish emergency measures to clarify the role of law enforcement agencies.	Temporary or emergency measures introduced by the DSA legislative framework will help mitigate the risk of excessive interventions by public authorities. Such measures would consist of temporarily disabling user-generated content due to its alleged illegality, but only for strictly prescribed periods of time. Temporary restrictions cannot go beyond this duration. This time window could be used for obtaining a judicial assessment of allegedly illegal content. Temporarily disabling the content could be applied in situations where an infringement is time sensitive.

Adopt and enforce due process safeguards that are easily accessible and available to online users

Due to their far-reaching impact on users' fundamental rights, internal rules and procedures deployed by online platforms should be known, accessible, clear, and transparent. The DSA legislative framework needs to contain procedural safeguards that will prioritise users' protection over economic profit and innovation.

1. Establish mandatory notifications to the content provider.	The legislative framework should establish mandatory notifications sent to content providers, informing them that a complaint has been made against their content. Ideally, the notification should be delivered to content providers before any action is taken by online platforms. Platforms could respond to content -restriction requests by either forwarding lawful and compliant requests to the content provider, or by notifying the complainant of the reason it is not possible to do so.[7]

[6] Council of Europe (2018). Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries.
[7] Manila Principles on Intermediary Liability (2015). Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation. Retrieved from https://www.manilaprinciples.org/

2. Create a possibility to submit counter-notice.	The DSA package should give content providers whose content is subject to complaint the chance to submit a counter-notification ideally before online platforms take any action against their content . This measure will allow content providers to object to the complaint,and thus, to effectively exercise their right to a fair trial. The counter-notice also allows the content provider to clearly state that he is not the author of the shared content if that is the case.
3. Define an appeals procedure.	A platform's decision to remove content or to keep it online should be communicated to both parties involved in the procedure. The decision should provide reasons explaining why platforms gave effect to the notification or not. It should also contain an explanation of the rights of the content provider, and any possibility to appeal the decision. The right to appeal a platform's decisions as well as the possibility to submit counter-notice should be included in notifications addressed to content providers. The explanation should contain an exact description of next steps that involved parties can take and the order of events that will follow. The procedure should also specify the exact information that a counter-notice should contain in order to be valid.
4. Secure access to effective judicial remedy.	Judicial review must remain available, when dispute-settlement mechanisms prove insufficient or where the affected parties opt for judicial redress. This safeguard should be provided as a final instance, regardless of which notice-and-action mechanism is used.
5. Safeguard meaningful transparency reporting by online platforms.	Transparency reporting requirements for online platforms should focus on quality and not on quantity, such as for example offering only statistics on removal rates, as these figures alone can only serve as a point of comparison, rather than providing valuable information about how online platforms deal with user-generated content. We suggest that the following information be incorporated into online platforms' transparency reports and mandated by law: ➔ the number of all received notices; ➔ type of entities that issued them, including private parties, administrative bodies, or courts; ➔ reasons for determining the legality of content or how it infringes the platform's terms of service; ➔ whether the content was flagged by private parties, automated tools, or trusted flaggers. Transparency reporting should also include: ➔ concrete time frames for notifying the content provider before any action is taken; ➔ concrete time frames for filing the counter-notice; ➔ the exact time that will pass before the content is restricted, and the time frame for an appeal procedure;

	➔ the number of appeals they received and how they were resolved. Public authorities should make publicly available and in a regular manner the following comprehensive information: ● the number, nature, and legal basis of all content restriction requests sent to online platforms; ● actions taken as a result of those requests; and ● content restrictions based on mutual legal assistance treaties.

IX. CONCLUSION

The substantive and procedural safeguards proposed in this position paper should be enshrined in the DSA legislative package. We strongly believe that their implementation will lead to effective protection of users' fundamental rights and harmonise the framework for Notice-and-Action procedures. The current EU legal framework does not contain such protective measures and thus fails online users because it does not defend them against unlawful interference with their rights by private actors.

2. Human Rights Response to the Amplification of Potentially Harmful Legal Content

2. Human Rights Response to the Amplification of Potentially Harmful Legal Content

POSITION PAPER | SEPTEMBER 2020

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 2

II. PROBLEM DEFINITION 3

III. HOW OPEN CONTENT RECOMMENDATION SYSTEMS WORK 5

IV. POLICY RECOMMENDATIONS 5

Minimum legal safeguards to protect users' choice 6

User-centric transparency 8

Data Access Framework 10

V. CONCLUSION 11

I. EXECUTIVE SUMMARY

In recent years, there has been a scaling up of content that, while it may not qualify as illegal based on the national legislation of Member States, is considered "harmful" or undesirable, whether by online platforms, users, or public authorities. Open content recommendation systems that personalise users' experience significantly contribute to the amplification of potentially harmful content, including the spread of disinformation and misinformation. Recommendation systems significantly influence users' choices.

The information users receive has been filtered through the lens of what data-harvesting companies conclude are users' personal preferences, based on their previous behavior and choices on platforms or the evident preferences of those in their network. Importantly, what users experience is the result of strategic decisions taken under a profit motive for commercial purposes, implemented through algorithms behind the scenes without the awareness of users or the scrutiny of public authorities, and relying on data collection and analysis that flout the spirit — and often the letter — of privacy and data protection laws.

Algorithms determine what users will see, which information will be prioritised and what content will be excluded. Large online platforms increasingly rely on open content recommendation systems that systematically analyse patterns of user behaviour and create profiles to determine what information is more likely to engage a given user. In other words, large online platforms harvest data to determine what personalised content offered to a user will spur engagement and generate more data about a user. This can have a detrimental impact on democratic discourse, the diversity of information. and the right to privacy.

This position paper provides a problem definition, an analysis of the problem, and a set of recommendations for the European Union to achieve meaningful transparency and user control. The DSA legislative package supported by the upcoming European Democracy Action Plan should ensure that EU measures are systematic and apply horizontally to foster media freedom and pluralism, to provide safeguards for election integrity and against manipulation, to tackle disinformation, and to adequately support civil society.

The three main areas of our recommendations are:

1. **Minimum legal safeguards to protect users' choice**
2. **User-centric transparency**
3. **A meaningful data access framework**

A key component for this umbrella framework could be a set of horizontal transparency requirements, such as:

- ➔ **User-centric transparency measures;**
- ➔ **Transparency measures to enable scrutiny by public authorities;**
- ➔ **Data access for academia and civil society; and**
- ➔ **Specific requirements for open content recommendation systems in line with potential broader obligations for algorithmic decision-making systems.**

NOTE TO READERS

Please direct your queries or comments to the following Access Now policy team members:
Eliška Pírková (eliska@accessnow.org)

II. PROBLEM DEFINITION

Many platforms have strong or even dominant positions in particular markets, and use recommendation systems to disseminate content, determining what content is recommended and how — a position of great power and influence. Due to the enormous quantity of content being shared on online platforms, private actors have to rely on automation to decide what content will be made visible to whom. The automated decision-making underlying this process of content governance is based on online targeting systems.

Online targeting lies at the core of data harvesting platforms and it shapes users' online experience. Online targeting allows large platforms to try to determine and speculate on people's personal preferences and behaviours. Because they harvest an unprecedented amount of personal data, they are able to boost user engagement and derive profit by prioritizing or quantifying the popularity of certain types of sensational content, including potentially harmful content such as disinformation. In the hands of major players, the acts of content moderation and content curation have become a commodity[8] from which platforms generate profit. Increasing engagement means that users spend more time on the platform, and consequently share more of their data. People's responses to this content are then collected and fed back to the system in an iteration cycle.

Today's large online platforms have developed strategies to extract "the surplus value of user-generated data."[9] Because their business models require large amounts of data, their main goal is to become and remain an indispensable point of online communication. Companies such as Facebook or Google have become global platform-based superstructures revolutionising

[8] Gillespie, T. (2018). Custodians of the internet. Retrieved from https://www.researchgate.net/publication/327186182_Custodians_of_the_internet_Platforms_content_moderation_and_the_hidden_decisions_that_shape_social_media
[9] Cohen E. J. (2019). Between Truth and Power:The Legal Construction of Information Capitalism. Retrieved from https://cyber.harvard.edu/events/between-truth-and-power-legal-constructions-informational-capitalism

information gathering and social interactions. An important byproduct of their operations is data-hungry algorithms. Recent research findings reveal that online platforms and their content recommendation systems can contribute to the polarisation of opinions and attitudes online. At the same time, it must be noted that several conditions have to be fulfilled for algorithmic filtering to be effective in causing polarization. For instance, an important factor is the predisposition and political attitude of especially those users who are already at the edges of the political spectrum.[10] Thus, it cannot be simply assumed that algorithms are capable of polarising society on their own, though attempts to manipulate content curation to drive engagement have been clearly documented.[11] Since controversial issues in particular generate user engagement, these issues are more likely to be highly ranked by algorithms and thereby more likely to be visible to a larger audience on social media.[12]

Content recommendation is crucial for the growth and dominance of large platforms, and lies at the heart of their business models. At the same time, their dominant position guarantees them significant regulatory powers over users and their rights. Or in the words of Gillespie, recommendation systems are "a key logic governing the flows of information on which we depend."[13]

Open recommendation systems deployed by large online platforms are partially responsible for contributing to the spread and amplification of potentially harmful user-generated content. To quote a report published by Ranking Digital Rights, scale matters: the societal impact of a single message or video rises exponentially when a powerful algorithm is driving its distribution.[14] However, the majority of legislative and policy responses to this problem — whether developed by governments or companies — focus exclusively on the elimination of potentially harmful user-generated content instead of addressing how individual pieces of content achieve high impact through recommendation systems. This results in restricting legitimate speech and imposes the direct threat of online censorship without actually addressing the root of the problem.

Instead of following this path, the European Union should focus on creating a systematic set of legal and policy frameworks for automated decision-making systems, online platforms, and data-dependent business models that ensures the protection and promotion of freedom of expression and other fundamental rights. This should include addressing the algorithmic engines

[10] Birgit Stark, Daniel Stegmann, Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse. Retrieved from https://algorithmwatch.org/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf

[11] Filter bubbles refer to the distribution and usage of information and development around a single user through algorithmic recommendations, in which the individual user may be largely uncoupled from relevant societal discussions. On the other hand, echo chambers refer to communication situations where one is exposed only to opinions that agree with their own, thus one is never alone in an echo chamber (Stark, Stegmann, 2020).

[12] Birgit Stark, Daniel Stegmann (2020). Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse. Retrieved from https://algorithmwatch.org/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf

[13] Gillespie, T. (2018). Custodians of the internet. Retrieved from https://www.researchgate.net/publication/327186182_Custodians_of_the_internet_Platforms_content_moderation_and_the_hidden_decisions_that_shape_social_media

[14] Nathalie Maréchal, Ellery Roberts Biddle (2020). It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge: A Report from Ranking Digital Rights. Retrieved from https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/

that drive the content distribution across platforms, and which amplify disinformation and other forms of potentially harmful legal content.

III. HOW OPEN CONTENT RECOMMENDATION SYSTEMS WORK

In general, content recommendation systems enable platforms to personalise what each user sees and to decide which content gets amplification and higher visibility, based on the profiling of users. Facebook's News Feed or YouTube's recommended videos are the results of content ranking derived from the information platforms have about their users. In practice, content recommendation systems generate individual rankings of hosted content for a specific user or a group or users. The factors for ranking can include the level of engagement the content is generating among other users, the type of content, when it was shared, or how users have interacted previously with similar content. The prioritised content displayed to the user is the one the system predicts they are most likely to respond to. Similar to systems for personalised and behaviour-based advertisements, content recommendation systems collect users' data to create digital profiles, assess similarities among users, and make inferences based on this data.

Many online platforms use content recommendation systems to reinforce their own policies which are stipulated in their Terms of Service (ToS). If the content does not comply with a platform's policies, the platform can down-rank such content, so very few people will see or interact with it. Another important way to categorise content recommendation systems is by the source of the content. Under this rubric, there are three main content recommendation models: open recommending, curated recommending, and closed recommending. For the purposes of this position paper, it is the open recommendation systems that are important because they provide recommendations from a pool of user-generated content only, without the editorial control of platforms. All large platforms use this type of content recommendation. A system where the default is to include user-generated content in the recommender's source pool, but where certain users or certain items can be excluded following ToS violations, is an example of an open system, and as we will show, such a system is the most prone to facilitating human rights abuses.

IV. POLICY RECOMMENDATIONS

The European Commission should ensure that legislative and non-legislative measures are systematic. In our view, many aspects of these issues will be covered by the Digital Services Act legislative package and potentially in initiatives on artificial intelligence and automated decision-making systems, including the European Democracy Action Plan. However, the relationship among the spending initiatives across other EU policies remains unclear.

The three main areas of our recommendations are:

1. **Minimum legal safeguards to protect user choice**
2. **User-centric transparency**
3. **A meaningful data access framework**

A key component for this umbrella framework could be a set of horizontal transparency requirements, such as:

- ➔ **User-centric transparency measures;**
- ➔ **Transparency measures to enable scrutiny by public authorities;**
- ➔ **Data access for academia and civil society; and**
- ➔ **Specific requirements for open content recommendations systems in line with potential broader obligations for algorithmic decision-making systems.**

We also note that some of the problems identified are strongly linked to Member State government propaganda and misinformation rather than being a problem of the information ecosystem.
Our recommendations aim to ensure fundamental rights safeguards for content recommendation systems. Algorithmically driven content curation in the hands of large online platforms is a powerful tool that can profoundly influence the opinions of online users. As a consequence, amplification of disinformation and other categories of potentially harmful content undermines users' ability to arrive at well-informed opinions and makes them more vulnerable to manipulative interference by external actors. The business models of online gatekeepers are built upon intrusive data practices and a persuasion architecture that can be used to manipulate and persuade people at a large scale. Personalisation of content may have a significant effect on the cognitive autonomy of individuals and interfere with their right to form an opinion.

It is essential that the EDAP initiative and the DSA package complement each other in order to fulfill their policy goals. Finally, the effective protection of users can be fully secured only if the GDPR legal framework is adequately enforced and implemented by all Member States.

Our key recommendations flow from our extensive research and experience with policy making:

Minimum legal safeguards to protect user choice

Personalized content recommendation systems used by large online platforms increasingly raise concerns over potentially negative consequences for diversity, the quality of public discourse, and privacy. The algorithmic filtering and adaptation of online content to speculated personal preferences and interests is often associated with a decrease in the diversity of information to which users are exposed.

We recommend that lawmakers:	
1. Enforce adequate compliance with existing legal frameworks protecting users' fundamental rights.	Any open content recommendationsystem has to comply with legal principles and norms for data protection, the principle of equal treatment and the prohibition of discrimination, as established by the existing legal regimes of Member States and the acquis communitaire of the European Union. The European Union should adopt measures that will secure the strict compliance of dominant online platforms with these legal standards.[15] Legal compliance will guarantee the mitigation of fundamental rights abuses stemming from users' "engagement on steroids," economic revenue as an underlying reasoning behind open recommendation systems, and the dominant market position of these actors.
2. Apply proportional sanctions for systemic violations of obligations listed in the legislative framework.	The legislative framework should establish measures that will enable national oversight bodies to enforce a prohibition on the deployment of open content recommendation systems at least until compliance is guaranteed and the fundamental rights of online users are sufficiently protected. The prohibition should be lifted by public regulators only if online platforms are able to sufficiently demonstrate their compliance with legal regimes. If they continue to use open content recommendation systems despite the prohibition, they should be subjected to proportional fines determined by the European Union. This model of prohibition is based on Article 58(2) (f) of the GDPR that enables Data Protection Authorities to impose a temporary or definitive ban on the processing of data in the case of systemic violations.
3. Guarantee conditional liability protection to online platforms for recommending illegal user-generated content.	Under no circumstances should the limited liability regime be triggered in cases of vaguely defined "legal but harmful" user-generated content. In this regard, the upcoming DSA legislative package should extend the conditional liability protection to user-generated content that is recommended via open content recommendation systems. The same requirements for conditional model of liability should then apply to platforms as in the case of hosting. Liability protection should not cover curated or closed recommendation systems, as they include content that was directly created or deliberately selected by platforms themselves.
4. Adopt meaningful transparency requirements into	The European Union should establish a minimum requirement for online platforms to keep logs of recommended content and criteria used for such recommendations so that they can be reviewed by users and by competent public regulators. The legislation should acknowledge that the nature of the record and structure of the record

[15] European Data Protection Board (2019). Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/leitlinien/guidelines-22019-processing-personal-data-under-article-61b_en

legislation that enable users' control.	should be adjusted to the needs of a particular audience. Users' access to a simple information summary should be enabled by platforms as default setting. Users should also be able to rectify or request the deletion of profiles. Online platforms should be legally obliged to provide information to users on where content comes from and reasoning about why it has been recommended.
5. Secure opt-in mechanism to personalised content recommendations systems by default on large online platforms.	The European Union should establish minimum safeguards for users' default settings to require an "opt-in" to personalised content recommendations systems rather than the current default "opt-out." Platforms should design "consent" and privacy policies in a way that facilitates informed choice for users and is compliant with data protection laws. Users have to be able to exercise minimal control over recommendation systems that can be secured by an "opt-in" mechanism. Making content recommendation systems available via "opt-in" by default would be a desirable mechanism because even those users who are less aware of how these systems operate will not be treated less favourably. Those users who decide to receive content recommendations should be able to: ➔ Exclude certain content from their recommendations; ➔ Exclude certain sources of content from their recommendations;[16] ➔ Ask for profiles to be deleted; and ➔ Access the service even when refusing to use content recommendations, to ensure the opt-in is meaningful. Users should be able to do so in an easy and free manner, and at any time they wish.

User-centric transparency

Online platforms typically incorporate diversity into open recommendation systems simply to engage the user and increase their profits, rather than to promote democratic debate. Open content recommendation systems may also have unintended consequences from the perspective of broader societal objectives.

[16] Jennifer Cobbe, Jatinder Singh (2020) Regulating Recommending: Motivations, Considerations, and Principles, European Journal of Law and Technology, Vol. 10, No. 3. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3371830

To return agency and control back to users, and to empower them, we recommend that lawmakers:	
1.Ensure that users have access to profiling data that platforms hold about them.	This data should be made available to an individual in a comprehensible format and should also include inferences made about that individual. While the GDPR largely ensures this right, there is a need for effective and accessible procedures or interfaces for individuals to obtain this information easily. Users should also be able to rectify and delete their profile.
2. Ensure that online platforms properly disclose that a user is or will be subjected to algorithmic decision making, including personalised content curation.	Meaningful awareness enables individual users to opt out if they wish to do so. Users have to be able to exercise control over recommendation systems that can be secured by an "opt-in" mechanism by default.[17] Platforms should design consent and privacy policies in a way that facilitates informed users' choice, in line with data protection laws.
3. Ensure that content recommendation models are being adequately explained to users.	Explanation of the family of models, input data, performance metrics, and how the model was tested should be communicated to users in tangible and comprehensible language.[18] Such an explanation will allow users to contest the algorithmic decision-making and/or to opt out.[19] The right to oppose the use of automated decision-making systems should apply even if a human is involved in the process.
4. Ensure that algorithmic decision-making is properly explained to users.	An explanation of a particular decision in understandable language, including statistics that were used and a detailed explanation of the platform's policy behind the decision, should be available to users as a minimum requirement to ensure the contestability of automated decisions.

[17] Jennifer Cobbe, Jatinder Singh (2020). Regulating Recommending: Motivations, Considerations, and Principles. European Journal of Law and Technology, Vol. 10, No. 3. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3371830

[18] Lilian Edwards, Michael Veale (2017). Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. 16 Duke Law & Technology Review 18. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855

[19] The UK Information Commissioner's Office (2020). Explaining Decisions Made with AI. Retrieved from https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence-1-0.pdf

Data access framework

The greater the impact on public discourse that gatekeepers of fundamental rights have, the stronger the need for a solid legal framework that will establish robust data access for independent researchers. A meaningful data access framework will allow for research-based policy making and reinforce public scrutiny over gatekeepers' operations that directly impact users' fundamental rights. The legislative framework has to establish what specific data should be accessible, who can request or directly access it, and who should gather those datasets, how they should do it, and who should check them before disclosure. Data protection authorities should provide guidance on how to ensure this access in a way that is compatible with the GDPR.

In order to safeguard research and evidence-based policy making, we recommend that lawmakers:	
1. Safeguard "public transparency by default."[20]	Predefined sets of data should be made available to everyone who requests access. Transparency by default includes exceptions that should prevent the violation of other competing fundamental rights. These exceptions should be decided upon and applied on a case-by-case basis.[21]
2. Enforce independent and transparent public oversight.	Independent public institutions should be responsible for verification and pre-processing of data in order to ensure that it is suitable for disclosure and that the process is fully compliant with the GDPR. It is crucial that public independent institutions that hold such a mandate are equally transparent about verification and pre-processing methods they apply to data before it is made accessible.[22] They should also identify what data is needed to ensure the required levels of accountability in the respective policy areas.
3. Enable data access in language that is useful for those who receive it and fits the purpose of the access request.	The data must be rendered useful for those who access it. In other words, it must be ensured that it is interpretable in various ways. A data access framework should ensure that useful data is presented to those who request access. Hence, access can take different forms, including aggregated statistics or more granular datasets.

[20] Jef Ausloos, Paddy Leerssen, Pim ten Thije (2020). Operationalizing Research Access in Platform Governance. Retrieved from https://algorithmwatch.org/wp-content/uploads/2020/06/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf

[21] Jef Ausloos, Paddy Leerssen, Pim ten Thije (2020). Operationalizing Research Access in Platform Governance. Retrieved from https://algorithmwatch.org/wp-content/uploads/2020/06/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf

[22] Jef Ausloos, Paddy Leerssen, Pim ten Thije (2020). Operationalizing Research Access in Platform Governance. Retrieved from https://algorithmwatch.org/wp-content/uploads/2020/06/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf

4. Establish data access requirements for third party independent auditing of algorithmic systems.	Researchers, experts and civil societies should have access to all information necessary for the audit to be conducted, such as source code and datasets, performance metrics that enable independent substantive oversight over the self-regulation exercised by online platforms.
5. Secure sufficient resources and capacities for researchers and civil society organisations for building research- and evidence-based policy making.	A data access framework has to ensure that researchers and civil society organisations are well equipped and have sufficient resources and funding to conduct research in a particular policy area.

VI. CONCLUSION

To achieve content diversity, the European Union should create the conditions under which users can find and choose between diverse content themselves instead of simply supplying a diversity of information based on criteria determined by platforms. Meaningful transparency of content recommendation systems, embedded in broader rules to empower users and ensure fundamental rights safeguards for automated decision-making systems, is absolutely essential in achieving this goal.

This position paper contains the most fundamental requirements and digital rights safeguards that should be applicable to content recommendation systems. While these policy goals should be addressed primarily by the DSA legislative package, some are subject to data protection enforcement and some pose a question for the broader regulation of automated decision-making systems. Access Now believes that the overarching issues across a number of regulatory sectors can be solved if the European Union establishes a human rights response to the amplification of potentially harmful legal content.

3. Proposal for Effective Oversight Model within the DSA Legislative Framework

3. Proposal for Effective Oversight Model within the DSA Legislative Framework

POSITION PAPER | SEPTEMBER 2020

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY **2**

II. PROBLEM DEFINITION **2**

III. LEARNING FROM PAST MISTAKES: THE ENFORCEMENT OF THE GDPR **3**

IV. HYBRID MODEL OF THE DSA OVERSIGHT MECHANISM **4**

A: Network of independent national regulators 4

B: European DSA coordination body 5

C: European regulator enforcing procedural safeguards 6

V. POLICY RECOMMENDATIONS **6**

Network of independent national regulators 6

European DSA coordination body 7

European regulator enforcing procedural safeguards 8

VI. CONCLUSION **9**

I. EXECUTIVE SUMMARY

This position paper proposes the DSA oversight model that could deliver effective enforcement of the future legislative framework. The paper draws lessons from the General Data Protection Regulation (GDPR) and the current state of its enforcement across the EU. Developing effective enforcement of the DSA legislative framework that stands on mutual cooperation among independent national regulators in relevant sectors is an ultimate precondition that the EU needs to meet for holding the key role in governing large online platforms.

The three main areas of our recommendations are:

1. **System of cooperation and competencies of the network of independent national regulators at Member State level**
2. **Creation and competencies of the DSA coordination body at the EU level**
3. **Creation and competencies of a new European regulator on procedural safeguards**

NOTE TO READERS

Please direct your queries or comments to the following Access Now policy team members:
Eliška Pírková (eliska@accessnow.org)

II. PROBLEM DEFINITION

The DSA legislative package will impact several regulatory issues, from disinformation to consumer protection, transparency and data harvesting business models of large online platforms, and fundamental rights, including data protection and the right to freedom of expression online. Due to its large scope, this is an extraordinary opportunity for the European Commission to develop an effective model of platforms' governance that prioritises fundamental rights protection of online users and serves the larger societal benefit.

The European Commission acknowledged that the regulatory issues to be covered under the DSA are subject to multiple divergent rules in different Member States due to uncoordinated regulatory efforts at the national level and the lack of proper information exchange among national regulators. Furthermore, platforms' governance usually involves numerous actors, from the private and public sector, civil society and academia. Each of these stakeholders have different responsibilities, levels of technical knowledge, and capacity. Finally, the public sector's enforcement is often weakened by procedural hurdles and delay tactics used by private actors and reinforced by enormous differences in the level of funding and resources.

Considering the level of complexity in setting up an effective oversight model, Access Now suggests the creation of a hybrid enforcement mechanism for the DSA legislative framework that contains elements of decentralised and partially centralised structure. The proposal is inspired by the enforcement model of the GDPRand learnings from its implementation.

III. LEARNING FROM PAST MISTAKES: THE ENFORCEMENT OF THE GDPR

In our opinion, the enforcement mechanism of GDPR should serve as a model for future DSA oversight systems and a good example from which to learn. The enforcement model of the GDPR consists of independent national Data Protection Authorities (DPAs) at the Member State level and the European Data Protection Supervisor (EDPS). The EDPS conducts independent supervision and is responsible for ensuring that EU institutions comply with the data protection obligations set forth in the respective framework applicable to them (e.g. Regulation (EU) 2018/1725, EUROPOL Regulation). All regulators are coordinated by the European Data Protection Board (EDPB). The EDPB is an independent European body, composed of national DPAs and the EDPS, that secures their mutual cooperation and makes binding decisions for the harmonised enforcement of the GDPR. In practice, the EDPB can provide general guidance to clarify the legal framework, provide advice to the European Commission in matters related to personal data, adopt consistency findings in cross-border data protection cases, and promote cooperation as well as best practices among national supervisory authorities. The supervisory authorities of the European Economic Area States are also members of the EDPB to participate in discussion with regard to the GDPR-related matters, without the right to vote or get elected as chair or deputy chairs.

Access Now has been monitoring compliance and the enforcement of the GDPR framework since its entry into application in 2018. Each year, we publish progress reports that map the state of play of the implementation of the Regulation. In our first progress report in 2019,[23] we emphasised that Data Protection Authorities, as the main supervising and enforcing authorities, play a critical role in the success or failure of the law. We also underlined that it is of the utmost importance that Member States guarantee and respect the independence of these authorities and provide them with increased financial and human resources. The same requirements are equally important for the authorities that will be involved in the future DSA oversight.

The enforcement system of the GDPR has been widely criticised since its implementation. Based on our findings however, the main reason why the effectiveness of the GDPR enforcement mechanisms is lagging behind is not due to the initial design of the system but rather its implementation. Concretely, it is the lack of resources and political differences hindering cooperation systems among authorities that is weakening the GDPR enforcement so far.

DPAs' low budgets and number of staff members mean that they are often unable to properly address a large number of complaints that have been filed or to carry out ex officio investigations. This means that inadequate budgets ultimately lead to lack of effective protection for individuals' rights. Furthermore, there are several troubling issues with the "one-stop-shop" mechanism that is supposed to serve both individuals and companies.[24] The high complexity of this system and the way it is designed results in "one-stop-shop" for companies and "three-stop-shop" for users. Even in the case of cooperation, one of the major obstacles in its effective functioning remains budget and resources. In order for any cooperation mechanism to be effective, the authority has to have

[23] Access Now (2019). One year under the EU GDPR: An Implementation Progress Report.
[24] Based on this system, users can bring a data protection complaint to the authority in the country where they live, even if the company against which they lodge the complaint has established its "main establishment" in another country. Meanwhile,companies can designate a lead authority which will be tasked with handling all complaints about them, regardless of where the complaint has been filed.This means that the lead authority has to cooperate with other authorities where people may file complaints.

enough staff members allocated to reinforcing the cooperation. Finally, no enforcement mechanism should place disproportionate weight on a single authority that is unable to cope with the number of lodged cases . This situation also increases the risk of forum-shopping, regulatory capture and external pressures, including from states, to force the regulator to act (or not act) a certain way.

IV. HYBRID MODEL OF THE DSA OVERSIGHT MECHANISM

The DSA oversight model that we are proposing is to a certain extent similar to the structure of the EDPB. It would include co-decision-making mechanisms which would vary depending on which sectoral areas are involved. Our recommended model for the DSA also follows the principles we described in our submission to the European Commission's White Paper on Artificial Intelligence.[25] Importantly, this would also mean decision-making via qualified majorities among regulators to ensure that no individual national regulator would be able to block the process entirely.

Due to the large scope of the DSA package, Access Now suggests a hybrid enforcement model that consists of three main layers:

A. A decentralised model at the Member State level: a network of independent national regulators shall be established that will be responsible for the enforcement of the DSA in their respective areas of competence;
B. A European DSA coordination body will be set up that could follow the structure of the EDPB, but with a broader range of competencies, to coordinate the national regulators;
C. A new European regulator will be created and tasked with oversight of procedural safeguards established by the DSA package, with the main focus on transparency requirements to be implemented by large online platforms.

A: Network of independent national regulators

Due to the wide scope and many regulatory sectors that the DSA package will ultimately impact, all relevant regulators over sectoral areas should be involved in meaningful enforcement mechanisms. The main regulatory bodies holding the oversight competence should be national Data Protection Authorities (DPAs), national audiovisual media regulators, consumer protection authorities, competition authorities, and telecoms authorities. Furthermore, there may be a need to create new regulatory bodies at the national level that will deal with specific issues, such as online disinformation or political advertising.

We suggest a decentralised model of oversight and enforcement at the national level. We strongly believe that a decentralised model based on the network of independent sectoral regulators will minimise the politicisation of the enforcement processes as well as prevent possible regulatory capture. Finally, it also ensures that people, users, and consumers can have easy access to their authorities to be able to exercise their remedy rights.

[25] Access Now's submission to theConsultation on the "White Paper onArtificial Intelligence - a European Approach to excellence and trust (2020).

B: European DSA coordination body

In order to safeguard mutual cooperation among Member States, the decentralised model of national independent regulators needs to be coordinated at the EU level. In this regard, we propose a coordination system with the structure similar to the data protection coordination mechanism represented by the EDPB. Such a body would be tasked with bringing together national independent regulators from relevant sectors in order to support their mutual collaboration on different areas regulated by the DSA package. Similarly to the EDPB, the EU DSA coordination body would be responsible for "meta-regulation" of large online platforms. The coordination body should act as an advisory board to the EU institutions.

In practice, the DSA coordination body would convene meetings of independent national regulators on a regular basis. The purpose of these meetings would be first, to discuss the concrete cross-cutting issues within the DSA legal framework that require expertise and enforcement by several independent regulators from different regulatory sectors. Second, the DSA oversight body should be equipped with a joint decision-making process to reach mutual agreement among independent national regulators on further actions. Consequently, the DSA oversight body should coordinate the implementation of these joint decisions across the EU. The coordinating body would have a broader range of competencies than the EDPB, as it should be tasked with supervising and verifying the independence of authorities. If the body considers a particular national authority to be controlled by a government or under regulatory capture, it could suspend its voting rights and participation in decision making processes within the coordinating body.

Furthermore, the DSA coordination body would be responsible for securing the involvement of civil society as well as private actors in discussion about concrete topics that require joint action by Member States. However, these stakeholders would not have direct decision-making power but would be involved via consultations or as public advisories. Any advisory role must ensure equal representation among NGOs, consumer groups, and private actors, and the selection process shall be conducted publicly.

To sum up, the DSA coordination body would hold the role of "central convenor."[26] Its primary role would be to coordinate discussion among independent national regulators with the goal of creating harmonised European rules for tackling different intersectional issues within the DSA framework. However, the coordination body should not fulfill the role of a single regulator at the EU level.

FInally, we propose the creation of the Expert Pool that would be administered by the DSA coordination body.[27] The Expert Pool would contain independent experts, coming solely from academia and with no conflict of interest, focusing on topics that fall within the DSA framework

[26] Ben Wagner, Carolina Ferro (2020). Governance of Digitalization in Europe A contribution to the Exploration Shaping Digital Policy - Towards a Fair Digital Society? Retrieved from https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/20200507_Governance_of_digitalization_in_europe.pdf

[27] Ben Wagner, Carolina Ferro (2020). Governance of Digitalization in Europe A contribution to the Exploration Shaping Digital Policy - Towards a Fair Digital Society? Retrieved from https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/20200507_Governance_of_digitalization_in_europe.pdf

and previously verified by the oversight body. Experts would be available to independent national regulators free of cost, in order to support their in-house capacity. The expense will be covered by the European coordination body. This expertise should be made available to national regulators upon request for a limited period of time, as required by the situation on the ground.

C: European regulator enforcing procedural safeguards

The final piece in the DSA oversight structure is the creation of an independent regulatory institution at the EU level that should supervise the online platforms' compliance with procedural requirements established by the DSA framework, with a strong emphasis on meaningful transparency. The clear mandate of such an institution and what action or investigative powers it could hold should be defined by the DSA package.

Importantly, the new regulatory institution should hold a function of "transparency facilitator."[28] This "transparency facilitator" will oversee platforms' compliance with technical and legal transparency measures, will be entitled to conduct independent audits and human rights impact assessment of platforms' content curation and content moderation practices, and will be tasked with enforcement of the data access framework established by the DSA package.[29] Furthermore, the regulator will be able to review wording and implementation of large platforms' Terms of Service, making sure that they are in compliance with international human rights standards. However, the regulator won't be able to receive and decide on individual complaints submitted by the platforms' users. This competence should stay in the hands of independent national judicial authorities.

V. POLICY RECOMMENDATIONS

Our key recommendations come from our extensive research and previous advocacy work in the field of data protection, especially during the GDPR negotiations. The following list of recommendations contains the main principles that the European Commission should take into consideration when designing the future enforcement model of the DSA legislative package.

Network of independent national regulators

The European Commission and Member States should empower national independent regulators to exercise effective enforcement of the DSA package across a comprehensive set of regulatory fields that are profoundly impacted by large platforms' operations.

[28] AlgorithmWatch, Putting Transparency at the Heart of the Digital Services Act: Why Data Access for Research Matters: How we can Make It Happen. (2020). Retrieved from https://algorithmwatch.org/en/submission-digital-services-act-dsa/
[29] For further details about the data access framework, please see the Access Now position paper "Human rights response to the amplification of potentially harmful legal content"included in this set of papers.

We recommend that lawmakers at the EU and member state level:	
1. Guarantee the independence of sectoral national regulators.	To function properly and to be able to adequately secure fundamental rights protection for individuals, Member States have to guarantee the independence of these authorities, both in statutes and financially. National regulators should be free of any political manipulation or regulatory capture by the private sector.
2. Increase resources of national independent regulators.	Member States have to increase financial and human resources (including skill and competence building) allocated to the independent national regulator responsible for sectors that will be impacted by the DSA package.
3. Increase cooperation among national independent regulators across Member States.	National independent regulators should increase cooperation between each other, including sharing information on cross-border cases and providing support for each other during ongoing interventions and investigations.
4. Provide one-stop-shop system to serve the user, not companies.	The European Commission should develop a cross-border cooperation that enables effective protection and users' fundamental rights. In practice, users should be able to lodge their complaints anywhere in the EU, based on their own choice. Complaints shall be heard and investigated, and decided by the regulator chosen by the user, no matter where a company has set its "main establishment."

EU DSA coordination body

The decentralised oversight model created at the level of Member States will require a strong coordination structure that will enable functioning information exchange and joint decision-making among all participating independent national regulators.

We recommend that lawmakers:	
1. Create a coordination body at the EU level with sufficient resources.	The coordination body at the EU level should have enough financial and human resources to exercise its coordination function properly. A strong secretariat assisting with daily duties should be the part of such a body. It should offer analytical, administrative, and logistical support to the DSA coordination body.

2. Clearly define its mandate and competencies in the DSA package.	The DSA package should specify the competencies of the future coordination body, including how its heads will be appointed. For independence, the European Commission should ensure that chairs of such a body will not be allowed to lead any national regulatory office in their respective Member States at the same time. Furthermore, the length of their mandate should be limited to a maximum of three years, renewable once. The European Commission LIBE Committee should hear candidates and designate the chair by vote.
3. Establish joint decision-making processes supervised by the DSA coordination body.	The DSA oversight body should be equipped with a joint decision-making process to reach mutual agreement among independent national regulators on further actions. Consequently, the DSA oversight body should coordinate the implementation of these joint decisions across the EU.
4. Enable the DSA coordination body to oversee the independence of national regulators.	In case the coordination body considers a particular authority to be controlled by a government or under regulatory capture, it could suspend its voting rights and participation in decision-making processes.

European regulator to supervise platforms' procedural obligations

Safeguarding meaningful transparency and accountability should lie in the core of the DSA package. Procedural safeguards that must be fulfilled by large online platforms need to be supervised by a newly established regulator that will be well equipped by technical means and resources to audit, measure the impact, and closely follow operations of large platforms.

We recommend that lawmakers:

1. Establish a new EU independent regulator with a clear mandate that will enforce transparency obligations established by the DSA package.	A new regulatory body should be solely responsible for monitoring the compliance of online platforms with the requirements for meaningful transparency. It should hold the following competencies: ➔ Conduct human rights impact assessments to ensure platforms' compliance with transparency safeguards established by the DSA legislative framework; ➔ Perform fundamental rights auditing of platforms content recommendation systems, advertising and microtargeting, and content moderation; ➔ Enable and supervise the data access framework dedicated to research for public interest.

2. Provide this regulator with sufficient resources.	The new regulatory body should have enough financial and human resources to exercise its coordination function properly.

VI. CONCLUSION

Large online platforms and the architecture of their business models have far-reaching consequences for society. Against this background, the co-regulatory soft approach has not proven successful to support innovation and ensure the protection of fundamental rights. Over the years, we have witnessed many bad examples of regulations aimed at large online platforms that shift the responsibility for protecting users' human rights on private actors. The DSA package can set an example of good law-making that will fill the existing regulatory gap, while placing users' fundamental rights at its centre.

The effective enforcement of the DSA package will require the participation of strong and independent public authorities at the EU and national levels. They must have the ability, resources, and powers to implement newly crafted measures across the EU. Importantly, the EU and Member States should equally play a key role in shaping regulatory dynamics by organising and advancing the implementation of the DSA package.