EUROPEAN DIGITAL RIGHTS

Platform Regulation Done Right

EDRi Position Paper on the EU Digital Services Act

European Digital Rights 12 Rue Belliard, 1040 Brussels www https://edri.org twitter @edri_org tel +32 (0) 2 274 25 70

Platform Regulation Done Right
EDRi Position Paper on the EU Digital Services Act

Published on 9 April 2020 in Brussels

Co-authored by:

Chloé Berthélémy, EDRi Policy Advisor
Jan Penfrat, EDRi Senior Policy Advisor

Layout by:
Rafael Hernández

This paper has received substantive input from EDRi members and observers over a period of eight months, in particular through written submissions by:

Access Now
Article 19
Electronic Frontier Foundation
epicenter.works
IT-Political Association Denmark
La Quadrature du Net
Panoptykon Foundation
Wikimedia Deutschland

Table of Contents

1. EXECUTIVE SUMMARY

The challenges of centralised platform monopolies, broken business models based on profiling, illegal online content and behaviour, and the spread of disinformation, are all legitimate public interest objectives.

The upcoming proposal for a Digital Services Act (DSA) is an opportunity for the European Union to decide how central aspects of the internet will look in the coming ten years, probably not only for Europeans but for the rest of the world as well. In this position paper, EDRi proposes cornerstones for an open, safe and accountable internet. This Position Paper outlines how the DSA can make the necessary changes to fix some of the worst outcomes of the advertisement-driven, privacy-invading, centralised attention economy that occupies big parts of the internet today.

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 like hate speech and defamation 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 try 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 privacy needs – while still being able to connect with and talk to all of their social media friends and contacts.

Key demands for successful platform regulation

1. Protect the limited liability regime of the E-Commerce Directive that has helped-make the internet great.
2. Require large commercial platforms to provide a way for users to report potentially illegal online content.
3. Give users more choice by making dominant platforms interoperable.
4. Impose strict transparency standards on large commercial platforms. Platforms should publish reports that inform policymakers, regulators and users about how they curate, moderate and remove online content and how they allow their customers to target online advertisement.
5. Require EU Member States to set up independent content moderation dispute settlement mechanisms that can settle disputes between users and with platforms – and make dominant platforms pay the bill.
6. Ensure that the terms of service of online platforms are transparent and understandable for users and fair in their application.
7. Establish a strong and independent European regulator that oversees and enforces compliance with the Digital Services Act – if needed, by way of dissuasive fines.

The second cornerstone is protecting an updated legal liability regime for hosting intermediaries with regard to user-uploaded content. Trying to use legal liability to push social media platforms 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 deter-

rent 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 fix everything that is broken in today's centralised platform economy but a combination of smart regulatory measures, as proposed in this paper, 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.

2. INTRODUCTION

"The Digital Services Act holds the potential to fix major flaws of today's hyper-centralised platform economy."

In this paper, European Digital Rights (EDRi) puts forward recommendations for the planned introduction of a new Digital Services Act (DSA) as well as a review of the EU's liability rules for online intermediaries. EDRi's proposals aim to uphold human rights in the digital environment, rein in the power of digital platform monopolies, better protect users, and reduce the spread of illegal content.

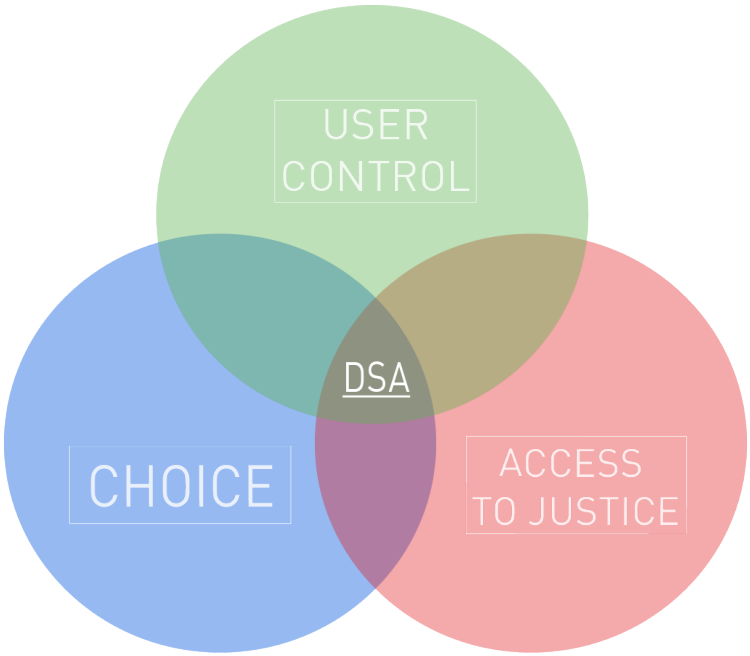
Acting as a foundation of the internet for two decades, the EU's E-Commerce Directive of 2000 contains rules that significantly affect people's ability to exercise their rights and freedoms online. The rules affect how intermediaries regulate and influence user activity on their platforms, including what users can and cannot say online. This is why reforming those rules has the potential to be either a big threat to users' rights and freedoms online or a major improvement of the current situation.

Up until now, the E-Commerce rules have applied horizontally to all sorts of illegal online content and behaviour, such as copyright infringements, hate speech, and child sexual abuse material. However, recently adopted legislation at national and European level imposes (or will impose) sector-specific rules for content removals. For instance, the recently adopted EU Copyright Directive and the draft Terrorist Online Content Regulation directly undermine long-standing key provisions of the E-Commerce Directive. Across Europe, politicians demand that online platforms to "do more" or "take more responsi-

bility" for their users' online conduct. Furthermore, the landscape of digital services that may or may not fall under current liability exemptions has changed drastically. Notably, cloud services and social media platforms have become very important players – some have gained significant market power and influence over individuals' rights, our societies and even the functioning of our democratic systems.

The DSA will have the task of modernising the current E-Commerce rules, introducing new regulatory measures without breaking the internet ecosystem, and ensuring full respect for fundamental rights. Why is that a challenge? The rules envisaged by the European Commission will inevitably affect a number of fundamental rights, including the freedom of expression and access to information, freedom of thought, conscience and religion, freedom of assembly and association, equality and the right to non-discrimination, the right to privacy and data protection, freedom of the arts and sciences, and the right to an effective remedy. This is why the final legislation should be very careful in its approach and mindful of international human rights standards.[1]

While doing so, it holds the potential to fix some major flaws of today's hyper-centralised platform economy. If done right, the law could help renew the internet's original promise: to be a decentralised, open network that enables everybody to communicate, create and participate in freedom, rather than a collection of digital silos, locking-in users and trading their most intimate personal data.



1 In particular Articles 11, 47, 51, 52 of the Charter of Fundamental Rights of the European Union, Article 10 of the European Convention for the Protection of Human Rights and Article 19 of the International Covenant on Civil and Political Rights.

3. TOWARDS AN OPEN, FLOURISHING INTERNET

The internet was originally built as a decentralised network with maximum resilience against shutdown and censorship. With a history in military research, its aim was to enable global communications that could not be easily prevented by any single adversary. Before today, the internet's uniqueness lay in its decentralised nature which avoided central points of attack or control. The social and economic benefits of this architecture were considerable: low costs of innovation, flexible ways to adapt and reuse existing technology for new services, and the freedom of choice for every participant in the network.

After the rise of centralised platforms in the 2000s, such as Facebook, Twitter and YouTube, however, internet companies started building advertisement business models based on the accumulation of massive amounts of personal data. In these business models, people are the product and their lives and most intimate moments are commodified and put up for sale to the highest bidder. Those businesses have turned the internet into a commercialised and centralised platform economy with strong network effects that lock in users and force them to follow arbitrary rules that only the companies control. As a result, most of what we do online today is mediated by a small number of service providers that cater to billions of users and exert fine-grained corporate influence over our fundamental rights and freedoms, such as freedom of expression and information.

Their combined user base amounts to more than 3.8 billion people, or half the world's population.[2] This causes multiple problems as platform companies develop and apply uniform, non-transparent content moderation policies to a large and diverse range of people, opinions and cultural norms.[3] At that scale, adapting to local realities and respecting very different jurisdictions and cultural backgrounds becomes a laborious process in which the platforms mostly fail.

Big social media companies often try to avoid legal liability by implementing procedures and technologies that tend to remove even legitimate content and risk censoring diverging and marginalised voices.[4] In fact, their content moderation practices often disproportionately affect already discriminated groups such as LGBTQI+ communities[5], women, migrants, people of colour, religious or ethnic minority groups and also human rights defenders[6], journalists, artists and political activists are more likely to see their online content removed[7] or shadow-banned[8] without reason given or access to redress.

Dominant social media platforms are also often unsafe for many groups at the margins. For them, it is hard to escape discriminatory and violent online behaviour, including harassment and violent threats. Whilst it is crucial to protect victims of aggressive online behaviour, there will be no effective, systematic response without addressing the above-mentioned business models of accumulating and trading personal data. The centralisation and commercialisation of the global communication space around a few platforms has created new barriers for many to exercise their rights and freedoms. This represents a big loss for rich and diverse public debate and therefore the democratic quality of our societies.

2 Based on data from Kepios DataReportal at https://datareportal.com/social-media-users.

3 Delia Paunescu, "Inside Instagram's nudity ban", Vox Recode, 27.10.2019 at https://www.vox.com/recode/2019/10/27/20932915/instagram-free-the-nipple-photo-facebook-nudity-ban-art-reset-podcast.

4 See for example Ben Bours, "Facebook's Hate Speech Policies Censor Marginalized Users", Wired, 08.14.2017 at https://www.wired.com/story/facebooks-hate-speech-policies-censor-marginalized-users, Chris Köver/ Markus Reuter, "TikTok curbed reach for people with disabilities", Netzpolitik.org, 02.12.2019 at https://netzpolitik.org/2019/discrimination-tiktok-curbed-reach-for-people-with-disabilities, and Anna Chung, "How Automated Tools Discriminate Against Black Language", POCIT, 05.03.2019 at https://peopleofcolorintech.com/articles/how-automated-tools-discriminate-against-black-language.

5 EDRi, "The digital rights of LGBTQ+ people: When technology reinforces societal oppressions", 17.07.2019 at https://edri.org/the-digital-rights-lgbtq-technology-reinforces-societal-oppressions.

6 UN Human Rights Committee, General comment No. 34, 12.11.2011 at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

7 Sam Biddle, Paulo Victor Ribeiro, Tatiana Dias, "Invisible Censorship. TikTok Told Moderators to Suppress Posts by "Ugly" People and the Poor to Attract New Users", The Intercept, 16.03.2020 at https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination.

8 Shadowbanning is the act of blocking a user's content on social media sites, in such a way that the user doesn't know it's happening. In the Terms of Service, platforms usually refer to their "right to limit distribution or visibility of content".

To make matters worse, the scale at which the centralised platforms operate creates highly problematic power imbalances: Users cannot escape the intrusive profiling of the advertisement-based mega platforms as the platforms make it impossible for users to choose alternative services without losing their contacts, online friends and social circle. This way, people are held hostage in systems designed to turn them into products by capturing their attention for micro-targeted advertisement.[9] And yet, users have no say in the elaboration of the platforms' so-called "community rules", while governments struggle to understand and control their impact on democratic processes. This diminishes users' bargaining power to demand changes to the mostly unaccountable and unreadable terms of service. What is more, the personalised advertising business model is incredibly intrusive and has major negative effects on people's privacy and data security.[10]

3.1. Addressing the manipulation business model

Enhancing online accountability of platforms cannot work without understanding the economic and commercial interests the players in the ecosystem have in encouraging harmful behaviour. Hate speech, disinformation[11] and other types of online content deemed problematic go viral and come out at the top of recommended content, as a result of the current "attention-seeking" profiling model of digital markets. Platforms, especially so-called social media, make profits by collecting, analysing and selling user data. Promoting controversial content that drives user engagement is key to the targeted advertisement-based business models of most of these platforms. Sensational, shocking or polarising content keeps people's attention and maximises their screen time, which in turn generates more profiling data and time to show advertisements – which is what creates profit for the platforms.[12]

Companies such as Facebook and Google use the personal data they collect to micro-target commercial, political and issue-based advertisements to individual users based on what is predicted to appeal to them and that they will subsequently engage with and click

9 Nicholas Thompson, "Our Minds Have Been Hijacked by Our Phones. Tristan Harris Wants to Rescue Them", Wired, 26.07.2017 at https://www.wired.com/story/our-minds-have-been-hijacked-by-our-phones-tristan-harris-wants-to-rescue-them.

10 Find out more about the industry's pervasive online tracking techniques at Panoptykon Foundation and Bits of Freedom: https://why-are-you-tracking.me.

11 Find out more about the industry's pervasive online tracking techniques at Panoptykon Foundation and Bits of Freedom: https://why-are-you-tracking.me.

12 In her piece "YouTube, the Great Radicalizer", sociology professor and Harvard associate Zeynep Tufekci uses the example of Youtube to explain how deliberately biased platform algorithms attempt to keep users attention fixed to their screens (and, in this example, Youtube) by pushing inflammatory or "radicalising" content, The New York Times, 10.03.2018 at https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.

on. Evidence continues to emerge demonstrating how these practices threaten democracy and exacerbate discrimination against users from already marginalised groups.[13] The New York Times investigated one of the most widely known disinformation stories of the US presidential election 2016 – namely that Hillary Clinton had committed election fraud – and found it to be purely driven by advertising revenue, which was successfully generated through and by Google ads.[14]

User lock-in → Promotion of controversial content →
Personal data harvesting → Big business from micro-targeted ads

> "As long as the chain of negative incentives is not broken up, no content removal or filter law in the world will prevent damage from the spread of problematic online content."

As long as this chain of incentives is left intact, no content removal or filter law in the world will be able to solve the problem and prevent damage from the spread of problematic online content. This position paper therefore focuses on addressing the chain of incentives and proposes solutions capable of fixing the centralised attention economy[15] in which today's platforms are caught.

3.2. Breaking up Big Tech?

Big Tech companies have become almost inevitable mediators for most of our online activities from messaging and sending birthday invitations to shopping and publishing our thoughts. The sheer size, reach and quasi-monopolistic power of many of the companies behind the most frequently used platforms causes enormous problems, which has led to many calls to break them up.

13 Latanya Sweeney, "Discrimination in Online Ad Delivery", Social Science Research Network, 28.01.2013 at http://papers.ssrn.com/abstract=2208240.

14 Scott Shane, "From Headline to Photograph, a Fake News Masterpiece", The New York Times, 18.01.2017 at https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html.

15 See Panoptykon, "10 Reasons Why Online Advertising is Broken", 09.01.2020 at https://en.panoptykon.org/online-advertising-is-broken.

Having a number of alternative social media platforms competing with each other for the best content moderation policies, the most healthy debating culture, or the most child-friendly suggestion algorithm would indeed be a great improvement to the monolithic, silo-based social media market we are seeing today. Yet it is not immediately clear whether and how companies such as Facebook or Google's parent Alphabet should be broken up: Should Facebook Inc. give up WhatsApp and Instagram, or sell out half of its 3 billion users to a competing network? Should Alphabet be prohibited from running Youtube or should it sell Android to another Big Tech company? What about Google's Play Store, email service, maps app, search, Chrome browser, and advertisement business?

> "The DSA can do more than just breaking up Big Tech because it can regulate the market ex ante and therefore prevent harm before it is too late."

What is more, enforcing powerful EU competition rules is slow and only works ex post, after the harm has been done.[16] Major antitrust investigations often take several years and by the time the European Commission is able to come to a ruling, the damage from the abuse of market power has already been done and the tech market has moved on. Even if a competition ruling is timely enough, the possible remedies are sometimes badly designed and therefore ineffective.[17]

The DSA can do more than just break up Big Tech because it can complement (ex post) competition law with ex ante measures and therefore prevent harm before it happens. That means the DSA can address not only abusive behaviour but also market failures, which are market distortions that do not necessarily stem from the abusive behaviour of a dominant company but still impede fair and open competition. What is more, the DSA can stimulate the plurality and diversity of the online ecosystem with the emergence of new providers and real alternative services and business models by lowering barriers to enter the market and regulating some of the most toxic activities of the currently dominant platforms.

16 Read further on what competition law has achieved when it comes to protecting digital rights, where it has failed to deliver on its promises, and how to remedy this in the following article: Laureline Lemoine, "The impact of competition law on your digital rights", European Digital Rights, 19.02.2020 at https://edri.org/the-impact-of-competition-law-on-your-digital-rights.

17 One famous example of such badly designed remedies with no visible effect on the market is the Commission's ruling on Microsoft's bundling of Windows XP and Media Player. In 2004, the EU's competition authority decided that Microsoft abused its dominant position in the operating system market to also win the market for media players, and forced the company to also sell an unbundled version of Windows. This unbundled version was sold by Microsoft under the name "Windows XP N" for the same price as the regular Windows XP. It only ever sold a few thousand copies, and the remedy had no positive effect on competition. A good timeline of the case T-201/04 was published by the Free Software Foundation Europe, who at the time intervened as third-party: https://fsfe.org/activities/ms-vs-eu/timeline.en.html.

So far, many of the EU's regulatory responses to the problems created by Big Tech only made them stronger. Because of the high costs related to their development and operation, obligations like copyright upload filters, anti-terrorism content filters, and disinformation self-regulation create a regulatory environment that only very large companies like Facebook or Google can afford to comply with. Smaller potential competitors meanwhile are struggling to keep up or don't even try to enter the market. Laws that were originally aimed at reining in Big Tech now cement their very dominance.

If breaking up Big Tech is not the way to go for Europe, what is? In the following pages, EDRi proposes a range of legislative measures that the EU should implement to limit the harm done by today's mega platforms. While no single measure will be enough on its own, the combination of strong rules will make the EU fit to compete in the digital age without compromising human rights online.

CHOICE

4. MODERNISE EUROPE'S INTERMEDIARY LIABILITY REGIME

"The DSA should foster an open, competitive and diverse online ecosystem with a wide range of online services and communication channels."

4.1. Proportionate rules to foster diversity and protect users

The scope of the E-Commerce Directive encompasses a wide range of service providers, including commercial and not-for-profit platforms as well as online marketplaces. Depending on the type of activities carried out by a platform, very different challenges arise and therefore, different sets of regulatory requirements should apply. Buying a hairdryer online and being able to trust that it won't set your house on fire is not the same as posting your opinion about the ongoing elections in your country on social media and hoping it won't be censored. Conflating these different types of online activities under a single set of rules could be detrimental to both freedom of expression and consumer protection.

The DSA therefore should distinguish between content intermediaries (such as social networks or messaging services) on the one hand and online marketplaces (selling physical goods or services) on the other. Because many modern intermediaries combine both activities in one platform, such as Facebook offering a social network for individual speech and an online marketplace for selling goods, the distinction needs to be made per service and not per platform.

Since EDRi's mission is to defend and promote fundamental rights in the digital sphere, the following recommendations reflect the scope of our work and apply only to content

intermediaries. This also excludes mere conduit and caching services as defined by Articles 12 and 13 of the E-Commerce Directive.

Considering its potential impact on the internet landscape, the aim of the DSA should not be limited to simply supporting the Digital Single Market but also foster the creation of an open, competitive and diverse online ecosystem with a wide range of online services and communication channels. For that purpose, some of the provisions proposed in this EDRi paper should only apply to 'dominant' intermediaries, a term that the DSA should define as related to but independent from the criteria of 'market dominance' known in competition law. While there are various possible ways to define dominance in this context, EDRi proposes to consider an intermediary service to be dominant if it has several of the following characteristics:[18]

1. The service is unavoidable for users because (a) it has 'bottleneck power' – which means the capacity to develop or preserve its user base because of network effects which lock-in a significant part of its users – or (b) its positioning in the downstream market allows it to create economic dependency.
2. The service occupies a considerable size in the market, measured either by the number of active users or by the annual global turnover of the provider.
3. The service is integrated into an ecosystem controlled by the group or parent company it belongs to, and this ecosystem allows it to leverage market power from one market in an adjacent market.
4. The service occupies a gatekeeper role for a whole category of content or information.
5. The service has access to large amounts of high quality personal data, either provided by users or inferred about users based on monitoring their online behaviour, which have become indispensable for providing and improving a similar service. In addition, this data is difficult to access or replicate by potential competitors.

The determination of dominance should be made by the European regulator proposed in this position paper in a fair and transparent manner. The regulator should develop documentation of its decision-making process accessible to all stakeholders in order to increase predictability and legal certainty for potentially dominant intermediaries and it should review its decisions on a regular basis.

Limiting some of the provisions of the DSA to dominant players helps target legal

18 These characteristics are inspired by an ARCEP working document on possible definitions of systemic platforms for regulatory purposes, "Plateformes numériques structurantes. Eléments de réflexion relatif à leur caractérisation", December 2019. ARCEP is the French telecommunications regulator Autorité de Régulation des Communications Electroniques et des Postes.

obligations to where problems actually occur and supports the successful development of competing alternative services and business models, as well as ensuring a fair and proportionate responsibility not-for-profit and community-led platforms that are more respectful of users' rights.

4.2. Updated liability rules for hosting intermediaries

The E-Commerce Directive of 2000 has exempted intermediary service providers who offer mere conduit, caching and hosting services from being held liable for online content or behaviour of third parties unless they have "actual knowledge" of it. This limited liability exemption is widely recognised[19] as one of the key factors that allowed the internet economy to flourish in its early days and build things like e-mail services, website hosting, and messaging apps.

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. It 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. At EDRi, we have consistently advocated and continue to advocate against laws that push companies like Google and Facebook to replace our independent judiciary. 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.[20]

The DSA should therefore protect and uphold the limited liability exemption as enshrined in the E-Commerce Directive for all types of intermediaries. Intermediaries should only become liable for user-uploaded content if they refuse to remove content that has been declared illegal by a valid court decision. This does of course not prevent intermediaries from voluntarily moderating content on their platforms—something many already do at scale today.

Likewise, intermediaries should not be obliged by law to build and use general content

19 Thibault Verbiest, Gerald Spindler, Giovanni Maria Riccio, "Study on the Liability of Internet Intermediaries", 12.11.2007 at https://ssrn.com/abstract=2575069.

20 The Electronic Frontier Foundation (EFF) and Visualizing Impact provided a collection of examples of how content moderation practices on big platforms fail to take correct decisions about both the legality of content and its adherenece to the platforms own terms of service, see https://onlinecensorship.org. For hate speech decisions in particular see Article 19's Hate Speech Toolkit at https://www.article19.org/resources/hate-speech-explained-a-toolkit.

monitoring systems including stay-down mechanisms such as (re-)upload checks based on hash databases. 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.[21] Such an obligation would have inevitable detrimental effects on the ability of people to freely share and access content online.[22]

When intermediaries build voluntary stay-down mechanisms, those systems should be audited and reviewed by the relevant European regulator (read this paper's chapter on the regulator below), which should check their compliance with relevant data protection laws, international freedom of expression standards, and other EU laws. Regardless, the use of such mechanisms should never be mandated by law.

21 The CJEU provided the description in Scarlet v. SABAM and SABAM v. Netlog and ruled in favour of the openness of the Internet and against the permanent surveillance and filtering of all European networks.

22 A similar argument was made by David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, in the context of the EU Copyright Directive, see https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24298&LangID=E.

5. IMPOSE STRONG LEGAL OBLIGATIONS

5.1. Interoperability obligations for dominant platforms

"Interoperability is the act of making a new product or service work with an existing product or service: modern civilization depends on the standards and practices that allow you to put any dish into a dishwasher or any USB charger into any car's cigarette lighter."[23] The internet community, such as the Internet Engineering Task Force (IETF), has developed a number of open standards that allow different decentralised systems to exchange information, like email[24], instant messaging[25], and even social media services such as the Usenet[26] and IRC[27] which could arguably be regarded as precursors to today's Reddit, Twitter and Facebook.

In the past decade, many of these open services have been replaced by so-called 'walled gardens'. Walled gardens are platforms or services that deliberately lock in users into

23 Cory Doctorow, "Adversarial Interoperability", Electronic Frontier Foundation, 02.10.2019 at https://www.eff.org/deeplinks/2019/10/adversarial-interoperability.

24 The IMAP, POP3 and SMTP protocols for example.

25 The XMPP standard, for example, which was later complemented with OTR and OMEMO for end-to-end encryption.

26 The Usenet is a decentralised discussion system developed in 1980. It resembles a bulletin board system and is the precursor to Internet forums that are widely used today.

27 IRC is a decentralised protocol for group communication and discussion forums comparable to Slack or other business chats used today. It also allows chat channels, one-on-one communication via private messages and data transfer.

that specific platform or service in order to prevent them from freely choosing a competing offer. They do this through a variety of means, such as through an interface design that discourages users from leaving the platform, or by making it technically impossible for competitors to launch an interoperable service.

As a result of this lack of interoperability, Facebook users for example are unable to send messages to non-Facebook users or invite them to events. Users from competing social networks can neither connect to their peers on Facebook nor post on their timelines. As a result, everybody has to be on the dominant platforms because everybody else is, even if they might not provide the best offer, or if they treat users unfairly. It is not least because of this 'network effect' that Facebook was able to keep 3 billion people on its platform with no viable competition in sight.[28]

In order to limit the risks of user lock-in and the resulting network effects that artificially bind users to one dominant platform, the DSA should empower competing intermediaries to interoperate with dominant ones. As interoperability involves the transfer of personal data from one platform to another, users should always have the free and informed choice of whether or not they want to interconnect with users of other platforms. Hence, users must remain in control of their personal data by deciding themselves which functionalities and services (public posts, "likes", direct messages, events, etc.) they would like to share cross-platform. This would give people real choice and enable the creation of sovereign European digital services.

This kind of mandatory interoperability can be achieved in different ways:

(a) Minimal interoperability

The DSA could oblige dominant intermediaries such as social media platforms or messaging services[29] to provide a technical interface (also known as "application programming interface" or API) that allows users of competing providers to dock on to the dominant one and exchange information with it.

The vibrant history of the internet shows that enforcing this kind of minimal interoperability for dominant platforms is a realistic technical solution and is already used today, for example:

28 The example of Facebook is not the only one, but it is particularly striking: The network effect in social media is so strong, that even Google, one of the most powerful and well-resourced Silicon Valley heavy-weights, was unable to compete with Facebook despite all the market power it has in other markets. Google decided to pull the plug at its own social network Google+ in 2019 after previous failed attempts with Google Wave and Buzz.

29 The can exclude services for which interoperability would not help reduce network effects would not otherwise give users more choice, or would be technically not feasible.

- Twitter provides an API that allows anyone to tweet using third-party software or websites. It's a hugely popular function of the platform and the reason why Mastodon[30] users are able to cross-post to Twitter and vice versa.

- Between 2010 and 2015, Facebook provided open access to third-party chat clients which created a vibrant market for alternative chat apps able to communicate with people on Facebook, until it was shut down to force users back on Facebook's own Messenger.

- Banks in the EU are legally obliged to provide an API to third-party online banking and payment services so that customers can freely choose which financial platform they prefer to use to manage their bank accounts and make payments.

The advantage of this approach is that dominant platforms would not be limited in the kind of changes they can make to their systems in the future. If Facebook were to develop new functionality or add a new (dis)like button, it could – under the condition that this change is reflected in its public API and is publicly documented. In this way, competing platforms can adapt their systems and remain interoperable without too much burden on the dominant player.

The downside, however, is that dominant platforms retain power over how the API functions and have at least some incentive to use bad documentation or implementation in order to deliberately worsen the user experience on competing platforms. If this approach were to be chosen for the DSA, it would need to include strong oversight power and sanctions for non-compliance with the interoperability obligation.

(b) Active interoperability through common standards

With an additional obligation for active interoperability in the DSA, industry would have to jointly develop and agree on open standards and protocols for transmitting user content across different platforms. Just like the open email protocol SMTP ensures that any Gmail user can send an email to a Hotmail or Yahoo user, an open social media protocol could allow users on competing platforms to interact with friends and contacts on dominant ones like Facebook or Twitter.

This is not a new idea: Since early 2018, the World Wide Web Consortium, a global internet standardisation body, have successfully developed ActivityPub, an open, decentralised social networking protocol through which social networks can interconnect their

30 Mastodon is a micro-blogging service that competes with Twitter. Its open and decentralised technology allows it to easily interconnect with other services that permit interconnection.

users across platforms.[31] Today ActivityPub is used to connect millions of people across social networking[32], micro-blogging[33], as well as photo and video sharing platforms.[34] If the DSA would oblige large social media or messaging platforms to agree on a common social media protocol and use it to interoperate, users from different platforms would be empowered to use the social network of their choice without being forced to give up their whole online community and lose all their "friends" or "followers". Competing platforms would be able to develop completely new services docking on to or building on top of existing ones.

For both options, mandatory interoperability would drastically reduce the imbalance of power between platforms on the one side and individuals on the other. It would (re)empower internet users to interact across digital silos and allow them to choose their own online community and appropriate guidelines. An interoperability requirement would ensure that citizens do not sign up to dominant platforms just because there is no other way to communicate with their friends and participate in the social life of their local community, e.g. students at a university. It would also directly strengthen healthy competition among platforms and could even create whole new markets of online services built on top of existing platforms, such as third-party client apps or content moderation plug-ins.

While interoperability will not be the single solution for all of the platform economy's problems, it can – in conjunction with a strong DSA which challenges harmful advertising business models – be a bold step in giving EU citizens more power, autonomy and choice online.

"Mandatory interoperability for dominant platforms would give people real choice and enable the creation of sovereign European digital services."

31 ActivityPub is an official W3C recommended standard published by the W3C Social Web Working Group. It provides a client to server API for creating, updating and deleting content, as well as a federated server to server API for delivering notifications and subscribing to content. Read more at https://activitypub.rocks.

32 The open social network Friendica is interoperable with ActivityPub. Another example is Diaspora*, an interoperable social network that uses the open Diaspora protocol.

33 The popular micro-blogging service Mastodon is built using ActivityPub.

34 Both the Instagram alternative PixelFed and the YouTube competitor PeerTube use ActivityPub.

5.2. A mandatory notice-and-action mechanism

In order to provide users, civil society, journalists, fact checkers and others with an effective way of notifying an intermediary about potentially illegal content on their systems, large[35] commercial[36] intermediaries should be obliged to provide a publicly accessible notice-and-action (N&A) mechanism.

Such a mechanism should consist of an online notice form that provides a transparent way of alerting intermediaries to content or behaviour that is potentially illegal.[37] While intermediaries should be obliged to act following a prescribed procedure when they receive notices through this N&A mechanism, they should not become legally liable for specific pieces of content nor should they be obliged to take down content they do not consider illegal themselves. If intermediaries were exposed to the threat of legal liability whenever they receive a notice from a random user claiming illegality of a given piece of content, companies would likely err on the side of caution and remove content just in case to avoid that liability threat. Such a system would essentially privatise the general legality assessment of all online content by outsourcing it to Big Tech companies with no judicial oversight. As for most companies business interests take precedence over users' freedom of expression rights, intermediaries need to continue to be broadly exempted from such liability to avoid the over-removal of legal and legitimate online speech.

Intermediaries usually have little incentive or experience in making balanced legality assessments[38] that respect the fundamental rights of their users. EU legislation must therefore avoid pushing companies into enforcing vaguely-defined public policy goals such as "eradicating online bullying" or "fighting online hate speech". Simply privatising law enforcement powers without transparency and redress does not solve the challenges the digital transformation brings. Instead, it would grant even more power to private actors who already today are largely free from any pressure from users and competitors alike.

35 Large intermediaries could be defined by the number of active European users, annual turnover, or similar metrics.

36 Intermediaries should be considered "commercial" only if their primary intention is to generate profit. Blogs, forums and other community projects that generate revenue merely to cover their costs should not automatically be deemed commercial.

37 The limited liability regime as well as other obligations to remove online content should only cover illegal content. It should not regulate content that is legal even if that content is considered undesirable by some or may potentially risk being harmful under some circumstances. This should not prevent intermediaries from moderating legal content under their own terms of service, provided that those terms are fair and transparent as set out in this paper.

38 In the Telefonica/Promusicae case, the CJEU recalls that Member States should ensure that a fair balance is struck between the various fundamental rights protected by the EU legal order when implementing measures restricting the exercise of those rights. This "fair balance" required of Member States becomes impossible to reach when the decision is outsourced, particularly if EU law such as the DSA uses the threat of intermediary liability to shifts the balance of incentives of providers towards content removal, see http://curia.europa.eu/juris/document/document.jsf;jsessionid=92D8361EB0607969F07DA0952585CAF9?text=&docid=70107&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2968360.

> "The notice-and-action mechanism EDRi proposes enables both intermediaries and users to assess how to best deal with a specific piece of content that is potentially illegal."

Any N&A mechanism should protect freedom of expression by introducing a transparent and fair EU-wide due process for intermediaries when they take content moderation decisions. The N&A mechanism EDRi proposes enables both intermediaries and users to assess how to best deal with a specific piece of content that is potentially illegal. In combination with simplified access to legal redress in court (see chapter on dispute settlement bodies below), such an N&A system would provide a powerful tool against the spread of illegal content online. Reliance on the N&A mechanism should of course always be without prejudice to the rights of affected persons to take legal action in court. Every content decision taken by intermediaries must be proportionate[39] and contain clear instructions for affected persons on how to access legal remedies.

Sometimes online content or behaviour such as disinformation campaigns, the spread of conspiracy theories or politically extreme positions can have potentially adverse effects on some people under some circumstances, while being entirely legal. Some stakeholders describe such behaviour using the very vague term of "harmful content" in an attempt to justify its quick removal. EDRi believes that this term is misleading and dangerous as it pretends that this kind of content is somehow universally unacceptable or even illegal. Reality is much more complex, which is why such content is not illegal in the first place. That is also why the European Court of Human Rights[40] has emphasised6 that freedom of expression as an essential foundation of democratic societies is applicable not only to information or ideas that are favourably received or regarded as inoffensive or as a matter of indifference. On the contrary, freedom of expression also applies to content that offends, shocks or disturbs the State or any sector of the population. Regulating such

39 One single copyright infringement should not lead to an account deletion, for example.

40 See details in the case Handyside vs UK, European Court of Human Rights case 5493/72, 07.12.1976 at http://hudoc.echr.coe.int/eng?i=001-57499.

"harmful" yet legal speech with hard (EU) law with a view to removing or suppressing its appearance on the internet, would have grave consequences for freedom of expression, freedom to seek information, and other fundamental rights. The N&A mechanism of the DSA should therefore apply to illegal online content or behaviour only.

In order to prevent abuse of the N&A mechanism by notice issuers, for example with a view to taking down legitimate content an issuer may disagree with, the DSA should introduce sanctions for issuers who systematically and repeatedly issue vexatious or abusive notices.

Law enforcement authorities should not be allowed to make use of the 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. That's 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.[41] This implies greater risks of abuse and political censorship that serve partisan interests – for example critical opinions against the government.[42] 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.

Third party notices should always be verified by the intermediary for their validity based on a strict set of requirements defined by the DSA. Such requirements should include:

- 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;

41 Conor Lally, "EU anti-terror chief urges Garda to target online illegal content", The Irish Times, 06.07.2018 at https://www.irishtimes.com/news/crime-and-law/eu-anti-terror-chief-urges-garda-to-target-online-illegal-content-1.3555424.

42 La Quadrature du Net, "La loi haine anti-Macron?", 09.05.2019 at https://www.laquadrature.net/2019/05/09/une-loi-contre-la-haine-anti-macron.

- 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.

In order to make the N&A mechanism workable, the required online notice forms should be straightforward to use and easily accessible, including for people with disabilities. Intermediaries should not discourage people from using it by making explicitly inhibiting design choices for the user interface (so-called 'dark patterns' that manipulate the user to behave in the platform's interest).[43]

Intermediaries should employ sufficient personnel to be able to respond to the expected number of notices in a time frame appropriate to the size of the intermediary and the gravity of the infringement at stake (for example, child sexual abuse material and death threats should receive priority treatment compared to copyright infringements because they entail a clear, imminent and concrete danger to individuals).

Where possible, the N&A mechanism should also allow uploaders to issue a counter-notice, to defend their viewpoint and interests; except where such a counter-notice would conflict with an ongoing criminal investigation which requires to keep the decision to suspend or remove access to the content a secret. For example, child sexual abuse material should be made inaccessible as quickly as possible (and be followed by criminal proceedings against the uploader), while notices of alleged copyright infringements or defamation need to provide the uploader with sufficient time to react before the content in question is removed.

Based on the outcome of such an exchange of arguments, the intermediary can make a transparent decision on how to moderate the respective piece of content. It should provide both the notifier and the uploader with a reasoned opinion explaining the decision, avenues to contest its decision either before a dispute settlement body as proposed below or before a regular court.

An efficient N&A mechanism should include appropriate time frames for each step which depend on the type of content in question. It empowers individuals to inform intermediaries about potentially illegal content on their systems and creates a transparent and binding process for all affected parties (complainant, potential victims, uploader, intermediary) to seek remedies if necessary.[44]

43 A report by the Norwegian Consumer Council demonstrated how dark patterns in GDPR consent collection tools were deceptive by default. See https://www.forbrukerradet.no/dark-patterns.

44 One way of defining the different steps and procedures for each given type of content has been developped by academic researchers Christina Angelopoulos and Stijn Smet, "Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability", Journal of Media Law, 21.10.2016 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944917.

5.3. Transparency obligations

Any notice and action (N&A) mechanisms must follow transparent rules and need to recognise the rights of all parties involved: potentially affected persons, the issuer of a notice, and the uploader. The DSA should therefore include the following transparency requirements for intermediaries that remove content that is illegal or in breach of the intermediary's terms of service:

- As soon as an intermediary takes action regarding online content or behaviour that has been notified and subsequently deemed illegal or in breach of the intermediary's terms of service, the intermediary must inform the uploader or account holder about the reasons and the law or terms they violated, unless the intermediary has no way to contact the uploader. That information must include a summary or description of the content in question.

- If an intermediary receives a notice about potentially unlawful online content or behaviour, the intermediary must assess the respective content or behaviour under applicable law(s) before assessing it based on its own terms of service.

- The intermediary must explain to the uploader and – where known – the notifier how to object to the action taken by the intermediary using a valid counter-notice, and – where necessary – how to access further remedies, for example via the Dispute Settlement Bodies described in this paper or in national courts.

- Exceptions to the above obligations should only be permitted in cases where informing the uploader or account holder is either technically impossible[45] or risks impeding a criminal investigations for example into the publication of child sexual abuse material.

Many large intermediaries employ automated means of taking content moderation and curation decisions, and these algorithms are likely to become even more ubiquitous. However, algorithmic assessments of the legality of individual pieces of content alone cannot guarantee the necessary protection of users. To the contrary, these algorithms have proven to actively reinforce biases and discrimination based on gender, race, sexual orientation and other factors, similar to the biases and discrimination we see in our societies offline.

In order to ensure compliance of algorithms with fundamental rights requirements and to avoid automated discrimination, intermediaries using that technology should therefore be obliged to:

45 This could be the case when there is no possible channel of communication between provider and uploader and if the uploader is unknown or unidentifiable.

- Make their algorithms available for auditing and testing by the European regulator proposed in this paper. Similar to medicines or food, authorities should have the right to test and refuse the marketing of harmful products in the EU. The regulator only has a chance of effectively preventing harm from automated discrimination if it can verify the functioning of a given algorithm.

- Explain users subject to an algorithm's decision how and based on what data this decision has been taken, and how they can contest it. Without real explainability, people will remain powerless in the face of machine-based decisions that can have immense impact on their lives.

In addition, large commercial intermediaries (see definition above) should be obliged to publish regular transparency reports about their content moderation practices, including detailed anonymised information about the notices they receive, the removal of content, or the suspension of accounts. These reports should at a minimum contain information about:

- The number of all received notices under the notice and action system and the types of content to which they relate;

- The type of entities that issued the notices (private individuals, organisations, corporations, etc.) and total number of their notices;

- Information about the content's illegality or type of infringement for which it was removed;

- The number of appeals the intermediary received and how they were resolved; and

- The description of the content moderation model applied by the hosting intermediary that includes but is not limited to the number of staff employed for content moderation, including their location, education and language skills, as well as any algorithmic decision making which influences the content moderation process.

Alternatively, the DSA could introduce an obligation to provide the above-mentioned aggregated data through a publicly available real-time API instead of written reports. That would allow researchers, journalists and the interested public to more easily analyse and effectively evaluate the content moderation practices of the intermediary concerned. Such an API should be standardised by the European regulator to allow for comparability across providers.

> "Large commercial intermediaries should be obliged to publish regular transparency reports about their content moderation practices"

5.4. Fair and transparent terms of service

Companies have to respect human rights. "The activities of [private companies such as digital platforms] may have many implications on individuals' capacity to enjoy their human rights and fundamental freedoms, such as the right to privacy, protection of personal data, freedom of expression, freedom of thought, conscience and religion, freedom of assembly and association, freedom of the arts and sciences, right to an effective remedy, among others."[46] However, most content moderation decisions taken by online intermediaries which restrict freedom of expression today are taken on the basis of commercial terms of services rather than the law. Despite frequent mentions, platform companies rarely put the EU Charter for Fundamental Rights front and centre when applying their terms of services. So-called "community guidelines" therefore often ban or restrict online content which is lawful and/or protected by European human rights law, in arbitrary and unpredictable ways. In addition, in the case of dominant social media companies, users have no power to influence the rules that are applied to police their online behaviour.

In order to ensure that the terms of service of intermediaries are fair and transparent, the European regulator proposed in this paper should have the power to ensure that commercial intermediaries:

- Are transparent about the measures taken;
- Notify users when implementing restrictions;
- Be proportionate in their content moderation practice by minimising the impact of their measures to the content only, or the user's account in case of recurrent breaches; and
- Establish clear, accessible, intelligible and unambiguous Terms of Service in all languages in which the service is offered.

The EU should also make sure that none of its legislation, non-binding initiatives like codes of conduct[47] or other activities incentivise companies to over-remove content, but instead encourages them to respect the fundamental rights and freedoms of people in the EU.

46 Joe McNamee and Maryant Fernandez, "Fundamental Rights and Digital Platforms in the European Union: A Suggested Way Forward", in: Luca Belli and Nicolo Zingales, Platform Regulations How Platforms are Regulated and How They Regulate Us, 2017, available at: https://juliareda.eu/wp-content/uploads/2019/09/Reda2017_Platform-regulations-how-platforms-are-regulated-and-how-they-regulate-us3.pdf.

47 Read more on EDRi's website: https://edri.org/guide-code-conduct-hate-speech.

6. ENSURE OVERSIGHT AND ENFORCEMENT

6.1. A European regulator overseeing compliance with the DSA

New legal obligations for 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.

Given the number of new legal obligations intermediaries will need to put in place under the DSA—in particular dominant ones—an independent European regulatory authority should be tasked to oversee compliance with those obligations.[48] 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 intermediaries under 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.

48 The regulator could be either a new, specialised entity or part of an existing body, as so long as it is well funded, independent, and competent in the effective enforcement of the obligations under the DSA.

6.2. Fines and sanctions for non-compliance

The DSA should introduce a strong system of sanctions for intermediaries that breach their obligations under the Act. Examples for breaches would be:

- Insufficient documentation of the mandatory interoperability API that is necessary for competitors to allow their users to interconnect with a dominant product or service;
- Failure to put in place an appropriate notice and action system as prescribed by the DSA;
- Failure to provide users with transparent terms of service; or
- Failure to provide access for the European regulator to algorithmic decision-making systems.

Fines for non-compliance with the DSA should be proportionate and have a sufficiently deterrent effect for companies. Similar to GDPR, the amount of a fine should be based on a percentage of the annual global turnover of the infringing company and take into account the overall compliance of the company with its rules and obligations.

Further sanctions should also include the mandatory change of the infringing behaviour as well as financial remedies for the potential damage caused by it.

> "In order to facilitate access to legal remedies, the DSA should require Member States to establish independent dispute settlement bodies for users in their jurisdiction."

6.3. Accessible and independent dispute settlement bodies

Every day, vast amounts of user-generated content are uploaded on social media platforms and other intermediaries' systems. Even very large intermediaries like Facebook or YouTube fail to properly enforce their own content moderation rules and comply with the law in a consistent manner. They frequently remove legal and legitimate content and block users that have done nothing wrong, not least because their automated content verification filters are unreliable.

That is why EDRi has consistently argued that only courts of law should have the last word about the legality of online content or behaviour and that this power should not be

outsourced to private companies. In a society based on the rule of law, an independent judiciary is the only actor with the democratic authority and legal competence to interpret the law regarding the legality of a given piece of online content.

Yet, in a world in which there are over 500 hours of video added to Youtube every minute of every day, the traditional way for users to seek redress for wrongfully taken down content or for falsely blocked social media accounts, which means via a national court, is often not practical either. While some have successfully sued intermediaries such as Facebook or Twitter for content take-downs – mostly lawyers, politicians, and journalists – this approach is not realistically accessible for the overwhelming majority of users. It's too complicated, too slow, and too expensive.

In order to facilitate access to remedies for users in the face of overwhelmingly powerful platform companies, the DSA should therefore require Member States to establish independent dispute settlement bodies for users in their jurisdiction. These independent bodies should go beyond the voluntary scheme provided for by Article 17 of the E-Commerce Directive by serving as a tribunal system providing simplified legal procedures tailored to the nature of online content moderation disputes. Their constitution should be closer to that of regular courts than to the privately-run out-of-court system that was originally established for online retail disputes by the EU ADR Directive.[49]

The dispute settlement bodies' task should be to settle disputes between users as well as with all intermediaries regarding the legality of user-uploaded content and the correct application of terms of services when they relate to content moderation decisions taken by intermediaries. Their decisions should be binding on both intermediaires and users. They should be fully independent and composed of legal experts. They should enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law.

The dispute settlement bodies should not replace traditional courts but complement them such that:

a. People are more likely to be able to defend their freedom of expression online when it is infringed upon by a wrongful content take-down or account blockage; and

b. The traditional, procedurally more complex court system is not clogged with the large number of (often repetitive) online content disputes.

Because the need for such independent dispute settlement bodies is directly related to

49 The EU Directive on alternative dispute resolution for consumer disputes of 21 May 2013 focusses on the disputes between consumers and traders in online sales of products and services.

the business models and functioning of dominant social media platforms like Facebook, YouTube or Twitter, the financial costs for their establishment should not be borne by the public alone. Instead, the DSA should require companies that run those dominant platforms2 to financially contribute to a 'European Online Content Dispute Settlement Fund' to be managed by the EU. The fund should be sufficiently large to set up independent national bodies capable of effectively fulfilling their tasks as described above. The fund could be topped up with financial resources stemming from administrative fines imposed under the DSA. That way, the dispute settlement bodies would act independently from both the intermediaries financing them and national governments, similar to the independence of national courts.

"The Digital Services Act is a unique opportunity to fix the structural problems of today's centralised platform economy and promote an accountable and transparent internet platform regulation system. The EU can and must enable an internet based on user choice, control and access to justice."

- European Digital Rights