Digital Services Act Proposal

Recommendations for the EU Parliament and Council

ELECTRONIC FRONTIER FOUNDATION

Published 2021
A publication of the Electronic Frontier Foundation, 2020. "Digital Services Act Proposal: Recommendations for the EU Parliament and Council" is released under a Creative Commons Attribution 4.0 International License (CC BY 4.0).

Contact
Christoph Schmon, International Policy Director: christoph@eff.org
Media inquiries: press@eff.org

EU Transparency Register
805637038375-01

DSA Proposal

On 15 Dec 2020, the European Commission released a draft of the Digital Services Act (DSA), which will modernize the backbone of the EU's Internet legislation, the e-Commerce Directive. The DSA proposes new responsibilities and rules for how Facebook, Amazon, and other companies that host user-generated content handle and make decisions about billions of users' posts, comments, messages, photos, and videos. This could be an unparalleled opportunity to reinvigorate principles like transparency, openness, and informational self-determination, and EFF has introduced a set of EU policy principles that should guide the reform process.

Our initial assessment concluded that the DSA is a mixed bag with some promising proposals. Here, we take a closer look at the substance of the DSA proposal and propose concrete recommendations for the EU Parliament and the Council.

The Commission Got Many Things Right

Key pillars of the e-Commerce Directive kept intact

Most importantly, the Commission did not abandon core tenets that made the e-Commerce Directive a success and helped to keep the internet free: the country-of-origin principle, the ban of mandated general monitoring of what users post and share online (Article 7), and the preservation of the extremely important principle that, as a general rule (Article 5(1)), liability for speech should rest with the speaker and not with platforms that host what users post or share online.

Without these principles, freedom of information would be impaired and platforms would be pushed to proactively monitor how users behave, and to block and remove any content that is controversial.

Recommendation on liability and monitoring: The key pillars of EU Internet regulation should be preserved. EU Member States should not impose general monitoring obligations on platforms or restrict the freedom of platforms to provide services in the EU. Online intermediaries should continue to benefit from comprehensive liability exemptions. Any change of current liability rules should clarify that actual knowledge of illegality is, save for content that is manifestly unlawful, only obtained if intermediaries are presented with a court order.

Type and size-oriented obligations

We support the general idea of tailoring due diligence obligations to type and size, to help ensure that smaller platforms with less capacity and control over content don't face the same burdens as very large online platforms such as Facebook or Amazon (Section 4). The idea of different obligations for more powerful platforms is in line with the proposal for the Digital Markets Act (DMA), which presented a new standard for large platforms that act as gatekeepers in an attempt to create a fairer and more competitive market for online platforms in the EU.

The DSA Proposal differentiates between a variety of platform sizes and types: information society services, intermediary services, micro or small enterprises, hosting services, online platforms, and very large online platforms (and, in the DMA, gatekeeper platforms are added to the list). Such a nuanced system of asymmetric and platform-depending obligations seems most apt to have a "targeted effect" and can help avoid disproportionate obligations. However, further scrutiny is required to ensure that exceptions are made where appropriate and that compliance with a rather complex system does not turn out to be overly complicated in practice.

Recommendation on type and size-oriented obligations: The DSA's asymmetric approach should follow the principle of proportionality and avoid deterring small providers from offering services in or to the EU.

Fundamental rights and procedural justice

We appreciate the Commission's commitment to protect fundamental rights and the numerous elements of procedural justice under the DSA, such as options for users to report potentially illegal content and rules on how platforms must handle complaints submitted through their internal complaint-handling system.

We also welcome the Commission's decision to follow EFF's suggestion to establish a right to reinstatement of content and accounts that have been removed by mistake (Art 17(3)). We also support that the proposal puts limits on the scope of takedown orders issued by national judicial or administrative authorities (Article 8(2)(b)). Without such a rule, which demands respect for general principles of international law, one country's government could dictate what residents of other countries can say, see, or share online.

Recommendation on reinstatement of content and take-down orders: The procedural justice elements in the DSA proposal should be supported, in particular an option for the user to appeal. We also recommend approving the crucial clarification that the territorial scope of takedown orders should not exceed what is strictly necessary to achieve their objective, respecting principles of international law.

Regulation of process rather than speech

Finally, the Commission was correct to focus on the regulation of process rather than speech. The DSA proposal would help users to better understand how content moderation decisions are made, especially the role of algorithmic decision-making (Art 12). Before the proposal was presented, EFF stressed that algorithmic processes on platforms are not necessarily centered on satisfying users' needs, but rather on maximizing the time and attention people spend on a given website. We are glad to see that under the proposal users would have a right to learn about the main parameters used in recommender systems and a right to opt for a system that is not based on profiling (Art 29), though privacy-by-default protection is necessary. We also support transparency reports around content moderation and options for vetted researchers and relevant regulators to take a closer look at how platforms help shape users' online experience (Art 33).

The lawmakers should build on the transparency focus of the DSA proposal and improve it to achieve actual accountable governance. Terms of service and community guidelines entail the fundamental rules that determine what users are afforded to do on a platform, and what behaviour is constrained. Users of platforms should be notified whenever the rules that govern them change, asked for their consent to such changes, and informed of the consequences of their choice. They should also be provided with a meaningful explanation of any substantial changes in a language they understand.

Recommendation on transparency measures: The DSA's focus on transparency measures and its contribution to safeguard freedom of expression and due process in the form of procedural safeguards is the right approach for modern platform regulation, which should think about how to regulate process rather than speech. This approach should be supported and further improved in order to achieve accountable platform governance.

Improvements Are Necessary

Interoperability: the Commission missed the mark

The Commission missed the mark on giving users more freedom and control over their internet experience by failing to include interoperability obligations in the DSA proposal. Such obligations are only addressed in the proposal for the Digital Markets Act—and still insufficiently. If the EU wants to end the online dominance of a few powerful platforms, we need rules that enable users to communicate with friends across platform boundaries. Interoperability in ancillary services such as payment processing is nice to have, but not good enough. Article 6(f) under the DMA will mean that, for example,

Facebook might have to let a competitor offer its own payment processing service for Oculus apps, but can still block the competitor from offering social media networking.

A general interoperability obligation for platforms' core services would be a far better way to foster innovation and put users back in control of their data, privacy, and online experience. We appreciate that the Commission introduced a real-time data portability mandate into the DMA. However, data portability is only the low-hanging fruit of interoperability, as users can't take advantage of it unless they have and keep an account on the gatekeeper service (and are thus still subject to potentially abusive terms of service).

Moreover, such portability mandates have been implemented in several privacy laws, including the GDPR, but have had limited practical impact. Mandatory interoperability will help foster real privacy. As EFF has argued before in our Privacy Without Monopoly white paper, Interoperability will let developers build tools so users can easily move from one social media platform to another, talk to people on Facebook without needing a Facebook account, have new ways to protect their private data, and be in control of their Internet experience.

Recommendation on interoperability: Interoperability obligations related to platforms' core services should be introduced into the DSA: Platforms that control significant shares of a market and act as gatekeepers to that market should offer possibilities for competing, not-incumbent platforms to interoperate with their key features.

A "notice-equals-knowledge" approach will lead to overblocking

Reporting potentially illegal content online is often daunting in practice and some platforms don't provide meaningful notification options at all. At the same time, notice systems can be abused. The Digital Services Act is a chance to create a more fair and predictable notice and action procedure, and we support the obligation for platforms to "put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means" (Article 14(1)).

We appreciate that the DSA proposal does not follow in the footsteps of recent disastrous Internet legislation that has endangered freedom of expression online by introducing a fixed period for platforms to act against potential illegal activity. However, in the current form, Article 14 could still push platforms into the role of quasi-law enforcers—a role for which they are ill-equipped at best. Specifically, the notice and action mechanism provides that properly substantiated notices automatically give rise to actual knowledge of the notified content (para 3). Even worse, the DSA proposal makes clear that platforms may remove content using "automated means" (para 6). As host providers only benefit from limited liability for third-party content when they

expeditiously remove content they "know" to be illegal, platforms will have no other choice than to block content to escape the liability threat.

In this respect, the DSA proposal also fails to address the concerns that platforms, rather than courts, are increasingly becoming the arbiters of online speech. Instead of putting measures in place that guarantee that it is up to independent judicial entities, not platforms, to decide the legality of any other user's content, Article 14(3) follows an approach of "shared responsibility" between users and platforms: users are supposed to be equipped with expert knowledge when explaining the "reasons why the information in question [is] illegal content" (para 2(a)), while platforms and their moderators are supposed to possess the legal qualification required to judge whether content should be removed.

Modern rules on platform regulation should be based on the principle that actual knowledge of illegality is, save for content that is manifestly unlawful, only obtained through orders by an independent judicial authority. Modern rules should also acknowledge that mistakes happen, on both user and platform-side. Attaching actual knowledge to every substantiated notice will do the opposite. At the same time, it will solidify the dominance of big tech platforms—which tend to react to such regulation by removing legitimate content to ensure compliance.

In this respect, the DSA proposal failed to pay due respect to the rationale of the e-Commerce Directive, which emphasizes the concept "actual knowledge" as a decisive element for the question of whether a platform enjoys immunity for user-hosted content. As the General Attorney opined in Peterson v Google/Youtube:

> *...attention should be paid not to the fact that the provider would have known had it been diligent, but to what it really knew.*

By contrast, the DSA proposal seems to opt for the fiction that platforms know about the content even where this is factually not the case. Such an approach is not fit for practice and should be dismissed by EU lawmakers.

Recommendation on the impact of user notifications: User notifications should not automatically be treated as conferring actual knowledge or awareness about illegality of the notified content. The proposal will undermine, rather than foster, freedom of expression and inevitably lead to overblocking of highly contextual content. Article 14(3) should be removed, and general follow-up obligations under a notice and action system should be disentangled from the system of liability for third-party content.

Voluntary measures

A censorship push via a badly designed notice and action system may be accelerated by other provisions that could, in the current design, encourage more private censorship and the application of filter systems. We welcome the clarification that providers can undertake voluntary investigations and actions for legal compliance without being

stripped of the exemptions from liability for third-party content (Article 6 - "Good Samaritan"). We also welcome that those actions comprise measures taken by platforms to implement the legal requirements for terms of service enforcement.

However, as the DSA Proposal has not abandoned the nebulous distinction between passive and active host providers, taking voluntary actions in good faith neither guarantees nor precludes that platforms enjoy immunity for content that users upload and share online. Similar to private notifications by users, voluntary measures can lead to awareness about illegal content or activity and thus trigger liability consequences (Recital 22). The lack of legal certainty is exacerbated by the vague scope of such privileged voluntary measures: Recital 25 explains that online platforms must act in good faith and in a diligent manner, without explaining the standard for such diligence.

Recommendation on voluntary measures – "Good Samaritan": It is crucial to ensure that the DSA does not incentivize platforms to expeditiously remove as much content as possible in the hopes of warding off potential liability. For this purpose, we recommend clarifying the scope of privileged voluntary investigations. We also recommend addressing the risk of content over-removals presented by the interlink between knowledge about, and liability for, illegal content.

Content restrictions, ToS enforcement, and service misuse

There are other open questions and risks of inappropriate removals of user content:

For example, Article 12 requires providers of intermediary services to include information about content restrictions and act in a "diligent, objective, and proportionate manner when enforcing their own terms and conditions." However, the yardstick for such a proportionality test is not clear, and its practicality will be put to the test in situations where platforms face an abundance of substantiated user notifications.

The same problem arises in situations where platforms encounter a frequent display of "manifestly illegal content", which is content whose illegality is evident to a layperson (Recital 47), and thus are compelled to suspend user accounts (Article 20(1)). The DSA proposal also addresses the situation of "service misuses" due to the submission of "manifestly unfounded notices and complaints" (Article 20(2)). In this case, online platforms must, as a minimum, suspend, for a reasonable period of time and after having issued a prior warning, the processing of notices and complaints submitted through the notice and action mechanisms and internal complaints-handling systems. We support the approach of the DSA to include safeguards against unfounded notices, which can lead to abusive and false takedowns. Such measures are entirely missing under Article 17 of the Copyright Directive, which the DSA could help to complement.

For both situations of "service misuse," it will be important to be mindful of the user detriment that could occur if user accounts were suspended too quickly or if notices by users, who may well act in good faith, were dismissed as unfounded too easily. A case-by-case review as stipulated by Article 20(3), which takes into account all relevant

circumstances, is the right approach. However, for the question of unfounded notices, a difference should be made between repeated, often automated notices submitted by entities or persons with specific expertise related to the content in question versus complaints by individual users, who will often not possess such knowledge and will not be a position to understand the consequences of misjudging content as illegal. This is particularly true in the realm of intellectual property rights, as profit-seeking organisations of industry and of rightsholders can be awarded the status of a trusted flagger under Article 19. For those but also for other entities, it is not clear whether third parties other than online platforms can refer to the Digital Services Coordinator if trusted flaggers misuse the notice and action system.

It is a general shortcoming of the proposal that trusted flaggers are not limited to independent entities or public interest groups. Recital 46 reveals that law enforcement agencies and other government entities are considered potential candidates for trusted flaggers of illegal content, even though faith in such entities may not be warranted in situations where users' fundamental rights, which require a high degree of protection from government intrusion, are at stake.

Recommendation on the misuse of services: We support proportionate terms of service enforcement and proportionate safeguards against service misuse. However, more nuance should be added to the current text. Platforms should be consistent in how they apply those measures and users should not face hasty account suspensions. We have strong concerns about industry-oriented entities and governmental agencies being "trusted" flaggers.

Right to anonymity and user control

The DSA Resolutions of the European Parliament stressed that intermediaries of digital services should enable the anonymous use of their services to the maximum extent possible and wherever technically possible. However, the DSA Proposal does not affirm users' informational self-determination and how platforms should address the will of individuals not to disclose their identities. Platforms may fail to consider the devastating effects if they enforce the use of legal names, such as harassment of members of the LGBTQ+ community, sex workers, and victims of domestic abuse. Anonymity should be considered a user right and deviating terms of service be subject to fairness control.

There are other shortcomings that will solidify rather than rectify the current dominant surveillance business model of capturing users' attention that shapes our online environments so fundamentally. For example, users should not face profiling by default and should have a right to decide against algorithmically curated recommendations altogether. The Digital Services Act should not fall behind this standard, in particular when it comes to automated processes that produce negative effects on users (Article 22 GDPR). In general terms, the Digital Services Act should strive to better protect users from profiling and digital surveillance. For the purpose of digital advertising, users should have a right not to be subjected to pervasive profiling unless they genuinely opt

in. Privacy protection should apply by default and companies should comply with browser signals that refuse consent to tracking.

Recommendation on the anonymous use of services: The EU Parliament and Council should affirm users' informational self-determination. Users should have a right to anonymity and be empowered to have better control over their data and online experience.

Mitigation of risks and law enforcement

It's not necessarily a single provision that is problematic, but the interplay of several provisions that pose a risk that platforms will not be able to "hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." Such interplay can be best demonstrated by Articles 26 and 27, which impose due diligence duties for very large platforms to address systematic risks, including freedom of expression (which we appreciate).

Platforms are required to mitigate risks that occur as a result of their terms of service enforcement, user notifications, and measures allowing platforms to identify potential illegal content. Combined with the provisions on sanctions, such a model would create a strong incentive to proactively avoid the occurrence of risks, using measures that cannot be mandated by the letter of the law (such as automated systems), but are the most cost-effective way to comply with DSA obligations. In this respect, the non-defined requirements of acting "reasonable, proportionate and effective" do not give much guidance on how platforms should act in practice and fall short of human rights standards and related concerns about what is necessary in a democratic society.

Recital 58 explains that mitigation measures should avoid unnecessary restrictions on the use of the service and take due account of potential negative effects on the fundamental rights of the recipients of service. It it's crucial that such safeguards and others that avoid the intrusion of privacy or the use of upload filters are included in the operative part of the legal act. A co-regulatory approach in the form of EU Commission "guidelines" on how to mitigate systemic risks on online platforms (Article 27(3)) will not give enough orientation to platforms for when to act and when not to act.

Then, the DSA proposal addresses several situations where the type of content requires platforms to alert law enforcement authorities (Article 21) or where platforms face pressure from public authorities to remove content (Article 8). Governmental agencies can even be awarded the status of a trusted flagger (Article 19) to pinpoint to illegal content. The "improved ability of law enforcement and authorities to supervise and tackle online crimes" and improved coordination mechanisms (Impact Assessment) also bear the risks of ignoring access to the justice rights of users whose content is removed or whose data are processed by enforcement authorities. Minimum standards, such as independence guarantees for trusted flaggers, are missing in the proposal, as are national retention and confidentiality rules for law enforcement authorities. With respect to judicial or administrative orders to act against a specific item of illegal

content, reference is made to the requirements under national criminal procedural law, but not to due process guarantees under administrative procedural law.

With respect to Digital Services Coordinators (Article 38), the primary national authorities responsible for the application of the DSA, it should be ensured that Coordinators are truly independent and that they enter in dialogue also with entities other than law enforcement authorities, in particular public interest groups and representatives of marginalized groups.

Recommendation on risks assessments and mitigation measures: The DSA should contain human rights-oriented safeguards that address intrusive measures taken by platforms in response to self-identified risks or in response to requests made by law enforcement authorities.

International impact

The more platforms are pushed into an active role to check, censor, and report what users post online, the greater the need for ex ante safeguards and fundamental rights protections. We are concerned that the DSA proposal may follow the footsteps of recent disastrous internet bills, such as the French Avia Bill (declared unconstitutional), the Austrian draft law on hate speech (under Commission scrutiny), or elements of the German NetzDG (under constitutional scrutiny). These bills ignore fundamental rights in that they target services regardless of their place of establishment. They have spawned dozens of copycats throughout the world, including in countries with far fewer protections for speech, and human rights more generally. All of these bills require the appointment of a legal representative, who faces enforcement actions for non-compliance. The DSA proposal, too, comes with a wide territorial scope of application, as non-EU platforms that provide services to the EU must comply with the DSA and appoint a legal representative.

We support effective oversight and enforcement measures. However, we are concerned about the fundamental rights impacts of these provisions, and the risk that platforms, in particular smaller ones, stop offering services to the EU when facing such requirements, which could ultimately undermine users' access to information. We understand that the Commission intended to exclude "very small" providers, as explicitly stated in the impact assessment. However, by providing that all intermediaries that provide services to the EU must provide a point of legal representative (Article 11), the DSA proposal fails, potentially due to a drafting error, to include such an exception.

Recommendation on international impact: The lawmakers should take into account the potential negative ramifications for the protection of fundamental rights protection globally. Exceptions should be made for small and micro-platforms that are not based in the Union.