September 2020

Developers Alliance's Position on the Digital Services Act Package

DevelopersAlliance.org

policy@developersalliance.org

Developers Alliance[1] welcomes the opportunity to submit feedback to the European Commission's (EC) open public consultation on the Digital Services Act package.

The present position paper is structured according to the topics treated in the modules of the questionnaire. It offers our membership's perspective on the revision of the e-Commerce Directive and on other issues that the EC considers that "may require intervention at the EU level."

We're disappointed again to encounter a flawed questionnaire in a EC's public consultation. Despite the possibility to offer detailed input for certain questions in free text boxes, there are many leading questions, especially designed to obtain responses which should provide the evidence supporting a pre-decided outcome. Therefore we chose not to answer several questions (mainly in the section n ex-ante rules), and to present our views in a separate document.

1. General Remarks

While the trend towards a digital economy has been obvious for many years, the recent COVID pandemic has highlighted the tremendous benefits this evolution has brought. The ability for citizens of the EU to work remotely, receive critical health and safety information, for the government to convene at a distance, and for students to access remote education would have been impossible to achieve even a few short years ago. The ability of the digital economy to scale and adapt is an unprecedented advantage in times of crisis. Regulators must be extremely careful not to impede this ability to save lives and safeguard economic well-being by rigidly limiting the ability for developers and the ecosystem they rely on to react to change.

In June this year, we co-signed a joint industry letter[2] asking for an appropriate legal framework that will truly benefit European startups and scale-ups. Legal clarity is key to the future of our members.

We commended the joint statement of the D9+ Member states Group[3], which calls for maintaining and carefully modernizing the core principles of the e-Commerce Directive (country of origin principle, liability exemption for intermediaries and no general monitoring obligation), with special reference to a harmonized framework for notice and action mechanisms, "with measures that are proportionate to the nature and impact of the harm committed".

The joint industry letter also underlines that the DSA should not overlap with the Platform-to-business regulation (Regulation 2019/1150), which is currently being implemented by the Member States.

---

[1] Developers Alliance advocates on behalf of software developers and the companies invested in their success, to support the industry's continued growth and promote innovation.

[2] https://www.developersalliance.org/press-releases/2020/6/26/e4kqytgr5ckbuyq0dgjmj1mh69hza1

[3] Poland, Belgium, Czech Republic, Denmark, Estonia, Finland, the Netherlands, Ireland, Luxembourg and Sweden

The Key Points Of Our Position

DevelopersAlliance.org

policy@developersalliance.org

On the revision of the liability regime:

- Maintain the core principles that keep the internet open for everyone.
- Legal obligations should be clearly defined by a harmonized EU framework.
- The distinction between illegal and harmful content is essential.
- What is illegal offline should be illegal online and in the same sense, the enforcement limitations accepted offline should be valid online. One should not ask internet companies to solve deep-rooted societal problems.
- Acknowledge that technology has its limitations. Protection of fundamental rights, such as freedom of expression is quintessential in preserving democracy.

On the ex-ante regulation:

- It is essential to correctly identify the problems and the appropriate solutions.
- Competition policy is better suited to tackle specific issues.
- We don't see any evidence of a significant change within the online platforms' ecosystems that would require an urgent regulatory intervention before evaluating the effects of the P2B Regulation.
- Start-ups can succeed without depending on a large online platform. At the same time, many startups would not have succeeded without the opportunities offered by large platforms.

On governance and enforcement:

The Digital Single Market is still an objective to be achieved. The fragmentation and lack of coordination seem endemic.

1. How to effectively keep users safer online

Software developers, especially application developers, are keenly aware of the need to keep their users safe online and take significant measures to prevent and remove illegal and harmful content. This is done not only because customer satisfaction and well-being is important for any business, but because as users of services themselves they feel first hand the benefits of trusted services. Developers are not only entrepreneurs, but concerned citizens at the same time, ones that understand more than others the risks coming from access to information and connectivity brought by the internet and the challenges of keeping the internet a safe place for everybody.

The revision of the e-Commerce Directive represents the right moment to ensure an updated harmonized legal framework for online content. It should preserve the core principles that enable the open internet and its history of innovation, while protecting fundamental rights, such as freedom of expression, and minimizing the presence of illegal and harmful content.

Our members have already put in place many measures to fight illegal and harmful content, according to the legal requirements of the jurisdictions they operate in, but also on a voluntary basis. These measures are diverse, just as the business models and the size of businesses in the digital economy are diverse. The common denominator for all is the objective of fighting illegal and harmful content. Their expectation is that the DSA will provide them a harmonized and clear legal framework across the EU, which will help achieve this objective in an agile way. The new framework should take into consideration various challenges that arise when putting in place measures against illegal offering of goods and services online and content shared by users.

While the complex legal landscape is hard to navigate for big online platforms, the millions of EU developers seeking to reach global markets can find it overwhelming. It is increasingly difficult for internet companies to maintain one set of global policies, even an EU-specific one,

as they are continually forced to consider country-specific policies to determine illegal content. The high costs and the administrative burden for SMEs are obvious and act as a disincentive to expand their operations into other jurisdictions. Obviously a made-in-the-EU framework that disadvantages EU companies from competing globally is nobody's ideal outcome.

The management of online content is a similarly complex task, and the industry has invested heavily in both human and technical solutions - including enlisting users and partners in the fight. But while users can help, companies cannot rely entirely on user reporting, which could be incomplete, over-broad or purely abusive (bad actors trying to game the systems). In turn, the limitations of purely technical solutions mandate some form of human overview.

Automated detection and removal tools are not always accurate. Efficient internal complaint and redress mechanisms are essential in addressing potential errors and responding to users' problems - which means that regulation must accommodate human limitations in any proposed solutions.

Transparency is very important. We agree that users should be informed when their content was removed and/or their accounts blocked. However, detailed information on the reasons is not always appropriate, mostly in those cases when the removal was requested by enforcement authorities.

Transparency reports represent an important tool to inform the authorities and general public on the various activities related to removing content from an online platform. While that became the norm for large platforms, the administrative burden for small companies is not negligible, and they need flexibility in achieving this objective.

Cooperation with enforcement authorities is functioning well in general, as demonstrated by ongoing responses to direct requests or providing regular reports where required. Looking forward however, we remain concerned over the potential for disproportionately burdensome requests (especially where companies are small and resources are limited), and to the wider deployment of new technologies that enable full privacy protection, such as encryption.

2. The liability regime of digital services acting as intermediaries

The new EU legal framework should provide a clear and viable liability regime for internet intermediaries. It should apply in a consistent manner to all online platforms, in order to avoid the migration of illegal and harmful content to smaller platforms. The rules should, however, be tailored according to the digital services acting as online intermediaries.

The 'notice & action' mechanism should be effective and allow online intermediaries to respond in an agile way to content issues, while preserving thriving forums for access to information and connection, where users' fundamental rights are respected[4].

The notice should contain at minimum the following information:

- clear identification of the content by URL, video timestamp, or other unique identifier
- clear identification of the notifier, in cases where the nature of the rights asserted requires identification of the rights-holder
- the legal basis of the claim and an attestation of good faith and validity of the claim
- an acknowledgement from the notifier accepting their obligations in the process (e.g. acknowledgement that a copy of notice may be sent to the original content creator).

[4] https://medium.com/global-network-initiative-collection/the-dsa-an-opportunity-to-build-human-rights-safeguards-into-notice-and-action-by-emma-llans%C3%B3-e0487397646f\

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

Regarding **the responsibilities that should be legally required from online platforms**, the following are suitable for all online platforms, and should be implemented according to the activities they intermediate, their size and capabilities:

- maintain a system for assessing the risk of exposure to illegal goods or content
- have content moderation teams, appropriately trained and resourced
- systematically respond to requests from law enforcement authorities
- cooperate with national authorities and law enforcement, in accordance with clear procedures
- be transparent about their content policies, measures and their effects
- provide technical means allowing professional users to comply with their obligations (e.g. enable them to publish on the platform the pre-contractual information consumers need to receive in accordance with applicable consumer law)
- cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities.

Requirements that imply intensive efforts, especially from startups and small businesses perspective should be reasonable and proportionate. The policy objectives should be achieved in the least burdensome way. The following obligations are examples in this sense:

- request professional users to identify themselves clearly ('know your customer' policy)
- in particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law.

A legal obligation to "inform consumers when they become aware of product recalls or sales of illegal goods" would be disproportionate.

The regulation should provide incentives for cooperation with trusted organisations with proven expertise that can report illegal activities for fast analysis ('trusted flaggers'), but not impose a strict responsibility.

We oppose a legal requirement to detect illegal content, goods or services, which would be translated into a general monitoring obligation.

Imposing a legal obligation to maintain an effective 'counter-notice' system for users whose goods or content is removed to dispute erroneous decisions will only force platforms to become the arbitration mechanism for contested rights. The courts are the appropriate authorities to take such decisions, and not online platforms.

The obligations of cooperation with law enforcement should be aligned with the proposal for electronic evidence ("e-evidence") regulation. We reiterate our concerns regarding certain aspects of this legislative proposal, currently under negotiations. The mechanisms for data disclosure requests should be subject to prior oversight by an independent authority or judicial review and ensure proper safeguards for the internet providers.

Legal obligations should consider technology limitations and be carefully shaped in order to avoid over-reliance on automation or mandated automation. The prohibition on general monitoring obligations, as set out by art. 15 of the e-Commerce Directive, should be preserved and the "notice & action" mechanism should be the norm. Not all online platforms can afford sophisticated tools. Automated tools can indeed be efficient in detecting and removing illegal content, but even the most advanced machine learning algorithms are still imperfect. In many cases the context has a determinant role in differentiating the content that should be tackled. Current technology is not performing well in distinguishing various contexts. The risk of taking down legal content is very high and the regulation should ensure the appropriate safeguards for fundamental rights.

We underlined these risks in our position on the proposal for a regulation on preventing the dissemination of terrorist content. Certain obligations, like taking proactive measures or complying with removal orders within 1 hour, are not only disproportionate, but will force the hosting service providers to use automated tools. Together with other stakeholders we urged

the co-legislators to consider the unintended effects of such obligations, especially on fundamental rights of European citizens, calling on them to carefully assess if these will ensure that the regulation will achieve its objectives[5].

DevelopersAlliance.org

policy@developersalliance.org

The country of origin principle is extremely important for startups and small businesses. It enables them to expand and scale up quickly in new markets, without costly adaptations to different laws across the Member States. The principle should be maintained as such, not weakened or replaced with a country of destination principle.

The legal requirements should be tailored to the specifics of the digital service's role as online intermediary, online platform, or something else. Search engines, web hosting services, DNS services, or cloud providers are more constrained, including on a technical level, in managing shared content. Cloud providers are a good example of such limitations, as they are bound by contractual obligations and by inherent technical constraints of their role as cloud infrastructure.

The regulation should also take into consideration the emergence of services that offer enhanced user privacy (encryption & tokenization functionalities, private communication using anonymization or pseudonymization). These cases may place limits on what is practical or appropriate when compared to completely unrestricted public systems.

With regard to the rights and responsibilities of other entities (public authorities and other interested third-parties, such as civil society organisations), we see their role in a joint societal effort to combat the dissemination of illegal content and attack the root of these problems. User education plays an important part in this process. More resources should be in place to support enforcement authorities, but also the entities engaged in education and raising awareness. All measures, beyond regulation, should be aligned in support of this objective.

Tackling harmful content while respecting fundamental freedoms is a real challenge.

As previously stated, the distinction between illegal and harmful content is very important. The latter, legal - but with a high potential of harmful consequences, should not fall under the liability regime.

It is impossible for regulations to identify in advance all situations when content becomes harmful. It's always an evolving and case-by-case evaluation. Platforms' policies already work hard to adapt themselves to establish guidelines on acceptable content. The same content that may be inoffensive one day for certain users could be perceived as harmful at some later date, or by other users.

This is no different from the offline environment. Following the policy objective of combating harmful content, the regulation should provide legal incentives for online platforms to ensure appropriate community guidelines and safeguards. Self and co-regulatory initiatives should be further supported by the EU and more online platforms, not only large ones, should be encouraged to participate in the process. The successful experience of the Conduct on Hate Speech and the EU Code of Practice on Disinformation should serve as a basis to continue this approach.

While we agree on all the proposed measures to address the spread of disinformation listed below, these are mostly relevant for large content-sharing platforms. It is important to pursue these objectives in a flexible way, in order to engage platforms of all sizes and to mitigate the risk of migration of disinformation to smaller platforms (targeted to certain audiences).

- Transparently inform consumers about political advertising and sponsored content, in particular during election periods
- Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with user complaints
- Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives

[5] https://www.developersalliance.org/press-releases/2019/12/2/80ongcxncao8cpuhn83asyjtllumio

- Transparency tools and secure access to platform data for trusted researchers in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it
- Transparency tools and secure access to platform data for authorities in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it
- Adapted risk assessments and mitigation strategies undertaken by online platforms
- Ensure effective access and visibility of a variety of authentic and professional journalistic sources
- Auditing systems for platform actions and risk assessments
- Regulatory oversight and auditing competence over platforms' actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on the manipulation and amplification of disinformation.

In relation to protection of minors, we support further actions at the EU level for strengthening the measures aimed to keep the internet safe for children and young people.

As the current context of the COVID-19 crisis showed, access to online education and online information and communication are essential for children and young people. The protection measures should be adequately shaped in order to preserve young people's access to the online environment, to avoid their isolation and to help them reap the benefits of access to educational, cultural and entertainment online services.

Given the international nature of many internet services which attract young people, we strongly urge that regulations already in place (e.g. COPPA in the US) are taken into consideration to avoid regulatory clash. We encourage regulators to collaborate internationally on child protection measures.

Enforcement authorities already possess a solid legal framework that allows them to impose special requirements to stakeholders when "a crisis emerges and involves systemic threats to society, such as a health pandemic." But **exceptional cases should not justify disproportionate measures and definitely should not become the norm**. For example, in the context of the COVID-19 crisis, special attention was paid to preserving the privacy of the users of contact tracing apps, in accordance with the GDPR.[6] Any provisions related to such situations should contain necessary safeguards and stipulate independent or judicial oversight.

Comments on the proposed measures for protecting freedom of expression:

The proposal for "high standards of transparency on their terms of service and removal decisions" should not offer bad actors the 'recipe' to game internet systems.

We agree that online platforms should be diligent "in assessing the content notified to them for removal or blocking" and "in informing users whose content/goods/services were removed or blocked or whose accounts are threatened to be suspended."

Maintaining an effective complaint and redress mechanism is also very necessary.

It is highly important that legal requirements would not push online platforms to overreact and remove content without a proper prior assessment. We reiterate the danger of relying entirely on automated tools. In this sense, we acknowledge the objective of ensuring "high accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts." However, technology and human limits should be recognized, so one should not impose an

[6] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

unattainable standard, particularly in the case of small platforms that cannot afford the resources large platforms have.

“Enabling third party insight – e.g. by academics – of main content moderation systems” should be pursued in full respect of GDPR and in a flexible manner. Online platforms should be allowed to choose the most appropriate mechanism for collaboration.

It is essential to provide users with clear content policies and appropriate mechanisms for reporting unlawful content. The online platforms should also have systems for reviewing flagged content and notifying users when their content is taken down. Internal redress mechanism is important too.

With regard to the algorithmic recommendations, the users of online platforms should be informed of the main parameters determining ranking and the reasons for their relative importance. Both the Platform-to-business Regulation and the Directive on Better Enforcement and Modernization of EU Consumer Protection Rules respectively stipulate that business users and consumers should be informed on the general parameters determining ranking as well as their relative importance.

We emphasize the risk of disclosing the detailed functioning of ranking mechanisms, including algorithms, to avoid misuse. There needs to be a clear line to avoid requiring businesses to reveal precise details about their business model. Recital 27 of the P2B Regulation[7] offers a clear explanation in this sense: “Their ability to act against bad faith manipulation of ranking by third parties, including in the interest of consumers, should equally not be impaired. A general description of the main ranking parameters should safeguard those interests, while providing business users and corporate website users with an adequate understanding of the functioning of ranking in the context of their use of specific online intermediation services or online search engines.”

The regulation should focus on providing the right incentives for online platforms to be compliant. Legal clarity and flexibility in achieving the regulatory requirements will prove more effective than sanctions. In any case, sanctions for non-compliance should be proportionate. Penalties are most appropriate where the infringement is systemic in nature.

We support a harmonized liability exemption for online intermediaries.

The liability exemption scheme should be maintained. This is a guarantee that the internet remains an open environment for everyone to use.

The updated scheme should reflect the development of online intermediary services and should address at least the following categories:

- Digital infrastructure services - which should be exempt if they meet the equivalent conditions set by the current art. 12.
- Cloud infrastructure providers, including Software as a Service providers - which should be treated as a separate category benefiting from a liability exemption due to the nature and the technical architecture of the services they provide. They are bound by contractual obligations to protect the privacy and security of their customer’s data and constrained by the inherent technical constraints of cloud infrastructure. They don’t have control over users’ content and have no legal authority to remove content. Therefore, third-party digital services providers that are using cloud or SaaS services should instead be responsible for complying with the legal requirements applicable to their content.
- Caching services, including search engines, which should continue to fall under a regime as set out by the current art. 13.
- Platform services, which should continue to benefit from a liability exemption, under the obligation provided by the current art. 14 “to act expeditiously to remove or to disable access to the information” upon obtaining knowledge or awareness of illegal activities or content. The revision should bring more legal clarity in eliminating the distinction between

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1150#d1e40-57-1

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

"active" and "passive" hosts. We reiterate the risks to fundamental freedoms, especially freedom of expression, associated with the prioritization of speed of removal and the pressure to take actions beyond the notice in order to mitigate the reappearance of that particular content or similar content.

The current disincentives for service providers to take proactive measures stem in particular from avoiding the risk of being labelled as "active" or being deemed to be aware of all of the content. Therefore, online intermediaries refrain from being overly proactive in the course of moderation activities or to remove content beyond notices.

Besides a clear "notice & action" system, the new framework should provide incentives for intermediaries to take proactive measures in content moderation.

It is important to stipulate that, in those cases where the service provider voluntarily reviews content in order to detect different types of violations of content policies, the service provider should not be deemed to have knowledge of the unlawfulness of all the content, the unreviewed content, or all the possibilities under which that content might be unlawful.

The notions of "active" and "passive" hosts are the source of legal uncertainty for service providers. Courts have brought limited clarity in defining them and recently it was acknowledged that certain notions used before became obsolete in the light of technological progress.[8] Therefore, the revision should set out updated terminology. We are of the opinion that notions such as "actual knowledge" and "the degree of control" will provide more legal clarity and certainty.

We strongly support the maintenance of the prohibition on general monitoring obligations.

General monitoring of the user-generated content would lead to the mandatory wide use of automated filtering tools. The risk to freedom of expression and privacy is extremely high.[9]

While currently there is no general obligation to monitor the information that users transmit or store, according to art. 15, the e-Commerce directive "makes room for specific cases" and allows Member States to require hosting providers to apply duties of care in order to detect and prevent certain types of illegal activities. The revision represents the momentum to clarify this, especially the recent policymakers' tendency to push the monitoring obligations in a dangerous direction.[10]

3. On "the gatekeeper power of digital platforms"

Preliminary remarks: The overall impression is that the Commission is already set to regulate "gatekeeper" platforms and is only searching for answers to back up its intentions. The questionnaire reflects this in that it fails to seek input on stakeholder opinions on what a gatekeeper is or how this designation is determined. The Alliance asks that the Commission establish evidence and invite comment on this position.

The online platform economy has an incontestable positive impact on the Single Market. We fully agree with the description of the role of online platforms in the European economy and the wide range of benefits of the online platform ecosystems for both consumers and their business users. Online platforms have a catalyst function for the integration of the Single Market[11], providing access to goods and services across the Member States and helping SMEs overcome persistent barriers and expand their businesses.

---

[8] Advocate General Opinion in joined cases Peterson vs. YouTube (C-682/18) and Elsevier vs. Cynando (C-683/18) highlights that "Optimising access to the content should not, in particular, be confused with optimising the content itself." (Para 83).

[9] https://cyberlaw.stanford.edu/files/Dolphins-in-the-Net-AG-Analysis.pdf

[10] https://www.law.kuleuven.be/citip/blog/to-monitor-or-not-to-monitor-the-uncertain-future-of-article-15-of-the-e-commerce-directive/

[11] Online Platforms, Economic Integration and Europe's Rent-Seeking Society: Why Online Platforms Deliver on What EU Governments Fail to Achieve

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

The online platforms' influence over the ecosystem is inherent in the deep integration of the many partners involved, and a necessity in ensuring balance and security of the business environment. Developers acknowledge the need to have checks and balances in place to the benefit of all. There are always advantages and disadvantages for the various players in such ecosystems. Frictions are inevitable, and solutions are found to balance different commercial interests, in an ongoing adaptation to the markets developments. For example, a successful app store needs to develop and maintain its offer of a large variety of quality apps and therefore the online platform is permanently interested to cultivate and improve its relationship with developers. A deterioration will only drive users away from the app store and both platform and developers will lose.

The technology industry is characterized by dynamic competition. Developers know that innovative ideas and new products always have a huge potential to disrupt the apparently stable market. This is what drives startups in working hard to present and promote their ideas. This is also what drives established companies in the market to work hard to optimize their products and to keep innovating. **"Innovation is Just a Click Away" is not a cliché, but the inspirational motto for the growth mindset of digital entrepreneurs.** Identifying issues related to barriers to market entry seems to be more an academic preoccupation than the reality start-ups and scale-ups face. Successful digital entrepreneurs are those betting on differentiation, presenting innovative products and delighting consumers, thus disrupting the existing offer. Newcomers are tapping opportunities by challenging existing large platforms and building marketplaces that can offer experiences tailored to the unique needs of a particular group of users.[12]

In the end, no matter the size of the company that develops an application, it is for the consumers to decide its success. There are plenty of examples in this sense, with the most recent ones in the context of the COVID-19 situation, when certain video conferencing applications swiftly "conquered" the market, imposing fierceful competition on incumbents and forcing large online platforms to adapt their products and to keep up with consumers needs and expectations.[13] This showed once more that innovation was a click away and the consumers chose the best products which respond to their needs, regardless of the size of the company behind the offers, be they incumbents or newcomers.

With regard to **mergers and acquisitions**, we underline that exit planning represents a normal mindset for the startup environment. For many serial entrepreneurs, the goal is to launch and scale an early business, then move on to new opportunities leaving others to grow the firm. Founders are always considering different exit strategies, other than IPO. The phenomenon of acqui-hiring, whereby established businesses find new talent through acquisition, is widespread in the technology sector, and should also be considered.

According to the PPMI report for the Observatory on the Online Platform Economy[14], of all companies acquired between 2013 and 2019, 70% of those companies originate from the U.S., and almost 20% from the EU. The State of European Tech 2019[15] also shows that "European tech M&A is dominated by exits to European buyers, which accounted for 60% of exit by deal count in 2019." These statistics speak for themselves.

We don't recognize systemic issues related to mergers and acquisitions and recommend instead a focus on reducing regulatory burden for start-ups and small businesses.

The EU Regulation 2019/1150 on platform-to-business relations ('P2B Regulation'), which started to apply as of 12 July 2020, provides important rules for online platforms' ecosystems. The transparency requirements represent an insightful tool for business users and consumers, but also for relevant authorities (e.g. competition authorities) to understand the outcome of certain mechanisms/processes, like ranking. At the same time, increased transparency obliges online platforms to enhance their awareness of the needs of their users.

---

[12] https://a16z.com/2019/09/11/platforms-verticals-unbundling/

[13] https://www.ftadviser.com/investments/2020/07/23/covid-disruption-is-breeding-innovation/

[14] https://platformobservatory.eu/state-of-play/power-over-users/

[15] https://2019.stateofeuropeantech.com/chapter/investments/article/european-exit-landscape/

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

The regulation also sets important obligations for online intermediary services intended to ensure fair commercial practices (e.g. notice periods, specific contractual terms, internal complaint systems). The first evaluation of the regulation, set out for January 13 2022 according to art. 18, is supposed to consider a series of aspects that fall under the DSA proposal.

In July 2020, after the P2B Regulation became applicable, the group of experts for the Observatory on the Online Platform Economy published three progress reports, "opening the debate to identify priority areas for further research, analysis and policy scrutiny".[16] Two of them treat aspects related to differentiated treatment and data. The conclusion of the Report on Differentiated Treatment[17] emphasizes the need for more transparency and oversight into online platforms' practices and recognize that P2B Regulation "provides a good starting point to facilitate the more concrete identification of forms of differentiated treatment that can be considered unfair and might, as such, need to be regulated." The Report on Measurement and Economic Indicators recommends that "the data generated by the internal complaint-handling procedures, as mandated by the P2B Regulation, should be analysed with a view to identifying and assessing any need for further public policy intervention." The expert group is also of the opinion that "it is desirable to keep monitoring the sector closely and conduct focused studies to scrutinise the impact of problematic practices."

The main conclusion of the PPMI survey (2019), regarding the business users' experience with online platforms is the following: "The most frequently reported causes of problems are technical problems, sudden changes to pricing and lack of transparency. Lack of transparency and offensive pricing strategies of online platforms may affect competition and the predictability of the market for the agents involved."[18] All these issues are properly addressed by the P2B Regulation.

We don't see any evidence of a significant change within the online platforms' ecosystems that would require an urgent regulatory intervention before evaluating the effects of the P2B regulation. Beyond this, current studies and investigations by competition authorities are already addressing specific complaints that relate to the issues mentioned by the inception impact assessment.

Regulatory intervention should address systemic issues that competition enforcement is not suited to tackle.

The focus on the size of the platforms is not the best approach. Setting out rigid rules based on fallacies is also not recommended (e.g. network effects[19]). Concerns related to the behaviour of certain online platforms, in specific areas/sectors, doesn't justify a drastic, inflexible and broad regulatory intervention. Moreover, the characteristics of digital markets, especially their dynamism due to the rapid pace of technological progress, call for an agile, future-proof intervention from regulators. Competition policy is the best way to investigate and address specific situations. Our feedback to the consultation on the New Competition Tool provides a detailed perspective on the proposed approach.

It is essential to correctly identify the problems and the appropriate solutions. We are not arguing that the online platform economy is a perfect place. There are complaints from consumers and business users about lack of transparency and fair treatment, but these are mainly issues related to certain sectors (e.g. e-commerce), and certain online platforms (e.g. Yelp's business users complaints on ranking and reviews[20]), or commercial disputes (e.g. the recent Epic Games' complaints about Apple's Appstore and PlayStore). We reiterate our view that the issues mentioned in the questionnaire are related to specific situations and sectors. Therefore, targeted investigations addressing individual companies or certain markets/sectors

---

[16] https://platformobservatory.eu/app/uploads/2020/07/Introductory_remark.pdf

[17] https://platformobservatory.eu/app/uploads/2020/07/ProgressReport_Workstream_on_Differentiated_treatment_2020.pdf

[18] https://platformobservatory.eu/news/measuring-the-platform-economy/

[19] https://hbr.org/2018/06/why-network-effects-matter-less-than-they-used-to

[20] https://slate.com/technology/2019/06/billion-dollar-bully-documentary-yelp.html)

represent a balanced approach and competition policy represents the appropriate way to intervene, assess the situation and provide remedies. We welcome the EC's engagement in this sense: "The work on the two impact assessments will be conducted in parallel in order to ensure a coherent outcome."

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

A cautious approach, backed by a solid impact assessment will avoid unintended negative consequences for European entrepreneurs. Any intervention, be it regulatory or by imposing remedies following investigations according to competition policy rules, have a direct effect on the targeted markets, but also indirect and unintended effects on all ecosystem players. Small software application developers continuously adapt their businesses to the developments of the markets they operate in. This happens in a natural way as the markets evolve, and encourages agile decisions and innovative approaches. They are used to the specifics of digital market dynamics, acknowledging that competition is always one click away and that at any time someone can engage consumers with a better product. But often they find themselves in situations where they need to take into account indirect (sometimes less foreseeable) effects of regulators' interventions that are focusing exclusively on the main parties and ignoring the rest of the players (e.g. the Commission Decision in the Google Android Case[21]). Regulators can avoid such unintended consequences by cautious approaches and solid impact assessments.

Any ex ante rules have the clear effect of modifying the market structure, thus forcing business model adaptations on different levels depending on the intensity of the regulatory intervention. Therefore we recommend a careful assessment of the potential structural issues that could be addressed by any kind of ex-ante intervention.

Specific Comments

On question 1 (**general statements**):

- The statements are general and imply a one size fits all approach, which is not suitable, given the huge diversity within digital markets.
- Certain statements may be highly relevant from the perspective of certain sectors. Also, the answers for certain statements may differ significantly from sector to sector.
- Certain statements reflect situations that are already addressed by recent specific regulations, and it's too early to perceive their positive effects (e.g. P2B Regulation provide rules related to the following statements: "the imbalances in the bargaining power between these online platforms and their business users" and "businesses and consumers interacting with these online platforms are often asked to accept unfavourable conditions and clauses in the terms of use/contract with the online platforms").
- The statement "large online platforms often leverage their assets from their primary activities (customer base, data, technological solutions, skills, financial capital) to expand into other activities" is based on a flawed perspective. Every business, no matter the size, in every economic sector, including traditional ones, is leveraging their assets to expand their activities and to be more competitive. There could be particular cases where dominant companies may act in non-competitive ways (according to the competition rules), but, as previously mentioned, should be tackled by competition policy and not rigid, one-size-fits all regulation.

[21] https://www.developersalliance.org/press-releases/2018/7/18/the-end-of-the-app-economy-golden-age

On the criteria for “gatekeeper” platforms:

- As mentioned above, issues that could be relevant from a “gatekeeper” perspective could be identified in different sectors or situations. Problematic market concentrations could be identified at regional or local level, or in certain areas/sub-sectors, not necessarily at EU level.
- Other proposed criteria represent general or vague characterization of certain situations, that could be difficult to establish and contestable (for ex. “Impact on a certain sector” or “They raise barriers to entry for competitors”).
- Certain criteria are ambiguous (for ex. “They accumulate valuable and diverse data and information”). Accumulation of data and information is not a problematic behaviour per se. All companies, not only in the technology sector, accumulate valuable and diverse data and information. The investments in advanced technology and the innovation around use of information are crucial for market success. The European Strategy for Data[22] emphasizes that: “the increasing volume of non-personal industrial data and public data in Europe, combined with technological change in how the data is stored and processed, will constitute a potential source of growth and innovation that should be tapped.”
- The criteria related to a large share of total revenue of the market/of a sector is probably the most relevant (assuming the market definition isn’t arbitrarily chosen). It is obviously the most fitted to quantification. This is, however, not enough in defining a “gatekeeper” role.
- We don’t see the need for a definition of a “gatekeeper platform.” A one-size fits all definition is obviously not appropriate. The ex ante regulation, if found to be necessary by evidence, should strictly address the identified structural issues, with focus on the problematic elements of those situations, without a general definition.

Question 4 of section III of the consultation doesn’t offer the option to disagree. The question “Do you believe that the integration of any or all of the following activities within a single company can strengthen the gatekeeper role of large online platform companies (‘conglomerate effect’)?” is not followed by a yes/no option as answer, but followed by an invitation to select different activities that are considered, in Commissions’ view, “to strengthen the gatekeeper role”. There is no free form text box which could allow, like for other questions, to present a different opinion.

Integration of different activities doesn’t necessarily have a negative effect, on the contrary, sometimes can increase the capacity of online platforms to offer diverse services to startups or scale-ups or to traditional, “non-digital” companies. Developers represent the main beneficiaries of the digital ecosystems. They rely on different integrated tools and services to reach their customers, to optimize their products or build new innovative ones, and to reduce their operating costs. Notable services, like online advertising and cloud computing are nowadays indispensable not only for developer businesses, but also for all companies with digital operations.

On “Emerging issues for businesses and business users of large online platforms”:

The questions should emphasize the structural nature of the issues that the Commission intends to identify. There’s a risk to collect specific, marginal problems, individual commercial disputes that are not enough evidence for an ex-ante regulation which will (re)configure entire markets.

Start-ups can succeed without depending on a large online platform. At the same time, many startups would not have succeeded without the opportunities offered by large platforms.

Startups face challenges as they scale, due to lack of resources and a lack of assets like patents to attract investors, even while fixed costs for market entry are lower than ever.

---

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

Startups don't need to build their own servers and data centers anymore, they have easy access to advanced technology, hardware and open-source software (including AI solutions), and different affordable services, like consumer marketing, advertising (provided by large online platforms) that allows them to quickly reach the audience and efficiently expand their business. Platform ecosystems like app stores are providing the most efficient way to enter markets and reach out to a global audience. Developers know that the fate of their applications on the market is always decided by consumers, as mentioned in the general comments for this section.

Developers that choose businesses models relying entirely on certain large online platforms assume the associated risks related to unforeseeable major changes in those ecosystems. They are aware that at a certain point they would need to adapt or to re-start from scratch. This is also valid for businesses in "traditional" sectors, like, for example, the SMEs that are part of industrial value-chains. Therefore we don't see the need for a special regulatory intervention in this sense.

The commission has presented no evidence or legal definition of a "gatekeeper role", so it is difficult to answer this hypothetical. Regulation in general should address more than just economic issues, but generally regulatory agencies specialize in particular economic segments and social policy areas. There is a real risk of trying to create generalized rules based on the specifics of a single company and then applying them arbitrarily to entire sectors.

With reference in particular to the questions 19-27, we strongly recommend a coherent legal framework at the EU level. **According to Better Regulation policy principles, the DSA should consider other relevant applicable legislation (like on a sectoral level) and stay consistent with other legislative proposals. The impact assessment should clearly identify and quantify the regulatory burden.**

Along the same line, setting up a new authority/new regulatory bodies will only interfere and overlap with the enforcement tasks of existing authorities. The DSA should rather offer a solid legal base for enhanced institutional cooperation between relevant authorities in the areas of consumer protection, competition, data protection, media regulation, market surveillance and so forth. A "swift and effective cross-border cooperation and assistance across Member States" is needed in this context.

The ex-ante rules should in no case overlap the scope of the new competition tool. Both proposals envisage tailored remedies, on a case-by-case basis, for similar issues.

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

Online advertising, in its various forms, and especially targeted advertising, represents an important support for developers to provide free or low-cost and high-quality services to the consumers.

This type of advertising represents the most efficient way to provide relevant adverts to consumers. It is also the most affordable marketing tool for startups and SMEs, such as those of app developers. Targeted advertising helps developers reach specific customer groups, limiting the display of ads to those who are most likely to respond positively. It would be less efficient to use contextual advertising. Targeted advertising lowers the costs and increases the availability of goods and services to consumers. Not all consumers can afford subscriptions, and the freemium revenue model represents the most popular way to monetize apps and mobile games.

The risk of misuse of the systems by bad actors should be put in balance with the benefits of advertising for both businesses and consumers. Cybercrime is a reality on the internet and it affects all parts of it, not only advertising ecosystems. All responsible entities in these

ecosystems are constantly joining their efforts in combating such crimes[23] and enhanced cooperation between industry and public authorities is further needed.

Placement of ads next to illegal content or goods, and/or on websites that disseminate such illegal content or goods could be prevented by rigorous policies and efficient enforcement tools. These should be developed by the services that help publishers monetize their content.

Enhanced transparency could prove useful in general for the online advertising ecosystem. As mentioned in our response to the UK CMA's Online Platforms and Digital Advertising Interim Report[24] we see the value of proposed improvements regarding transparency interventions in digital advertising markets. We also commended that some of the concerns related to the online advertising chains, including those related to algorithm changes, bids in auctions, or fees, may be addressed by the proposed code of conduct.

We fully acknowledge that consumers should be empowered to choose what ads want to see. App developers are implementing different technical solutions which provide them information and control. There are also useful solutions developed by the ad tech industry[25]. We are also of the opinion that consumers should be informed about the advertisers behind ads and why they are seeing certain ads.

On smart contracts

Smart contracts don't always qualify as legal contracts. In the case of those that do qualify as legal contracts under the applicable contract law, more regulatory guidance at the EU level could prove helpful, especially on the application of the Rome I and Brussels I Regulations, concerning the mutual recognition of lawfully concluded smarts contracts under the national jurisdiction, and also in relation to the consumer protection rules.

How to address challenges around the situation of self-employed individuals offering services through online platforms?

Freelance software developers can be found in the position of "self-employed individuals offering services through platforms".

We highly recommend that any measures intended to address platform workers should take into consideration the specifics of this particular sector of activity. A one-size-fits all approach may have unintended consequences for certain categories of professionals, such as designers, data scientists, programmers and software engineers. Concerns related to the situation of self-employed individuals in sectors like ride-hailing, food delivery, or domestic work are not necessarily relevant for freelance software developers. For example, the concept of collective negotiations is irrelevant in the case of freelance

A high degree of flexibility and autonomy is preferable for software developers, many of which prefer freelance contracts or other work agreements which usually include remote work options, part-time or flexible schedules or other specific conditions. This, combined with satisfactory incomes enable a better work/life balance. The cross-border aspect of their activities should be also considered.

At present there are no systemic issues or generalized concerns related to platforms intermediating freelance developer workforce that would require regulatory intervention at the EU level.

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

---

[23] https://www.iabuk.com/news-article/asa-launches-scam-ad-alert-system

[24] https://assets.publishing.service.gov.uk/media/5e8c80c2e90e07077c089ee3/200212_Developers_Alliance_Response_to_Interim_Report_NON-CONFIDENTIAL.pdf

[25] http://www.aboutads.info/choices/; http://www.youronlinechoices.com/uk/your-ad-choices

5. Governance of digital services and aspects of enforcement

DEVELOPERS ALLIANCE

DevelopersAlliance.org

policy@developersalliance.org

We commend the EC's acknowledgement that **"the 'country of origin' principle is the cornerstone of the Single Market for digital services"** and its importance for digital entrepreneurs.

The Digital Single Market is still an objective to be achieved. The fragmentation and lack of coordination seems endemic.

Ambitious startups and SMEs often encounter 27 different legal frameworks - without even leaving the EU. Rules at EU level are not always implemented in a consistent manner across the EU, there are inconsistent interpretations of those rules, complemented by national initiatives. These are not the expectations on entering the Single Market. For example, businesses shouldn't encounter separate compliance frameworks when putting products and services into the EU market or need to prepare separate transparency reports. A harmonized approach should be supported by common standards for compliance practices. Ideally these should be developed at the international level, as most of the digital services providers operate in a global environment.

The updated regulatory framework should reinforce cross-border cooperation mechanisms. This should be structured around clear objectives and set efficient processes and assistance across the national competent authorities. The supervision institutional structure should focus on the systems online platforms have in place, and transparency reporting should serve as the primary tool. Decision-making processes should be evidence-based, and include appropriate checks and balances and safeguards (e.g. independence of regulators).

Regarding the information that the competent authorities should make publicly available about

their supervisory and enforcement activity, this should be done in the spirit of good governance and transparency, allowing stakeholder participation in the regulatory process.

The responsible authorities should have adequate resources, including technical expertise. This should be complemented by active engagement with the industry, to properly understand the specifics of the markets or issues under supervision. The cooperation with civil society organisations and academics for specific inquiries and oversight is equally important.

There is no need to ensure specific supervision of digital services established outside of the EU that provide their services to EU users. The same rules apply to all services in the EU, therefore the same enforcement mechanisms should be applicable to all service providers that are operating in the Single Market, no matter their country of establishment.

A coherent approach is the ultimate objective, be it achieved through an enhanced cooperation or in a more centralized way at the EU level.