December 2020

Due Diligence Obligations in the DSA: DOT Europe Questions for Consideration

Over the past several months, DOT Europe[1] has observed lively and engaging discussions on the European Commission's forthcoming Digital Services Act (DSA).

Many different stakeholders in the DSA debate have identified specific issues they wish to address in the online ecosystem, and have floated suggestions on how to do so - ranging from transparency reporting, to a "know your business customer" obligation, to notice and action rules. Collectively we have often seen these various measures referred to as "due diligence obligations" for online service providers.

These measures are not necessarily new, and many online service providers currently make use of them on a voluntary basis to tackle different issues on their services. DOT Europe members have much to contribute to the thinking on the practicality and feasibility of possible approaches and to elevating these measures to EU-level due diligence obligations, for example in light of other legislative initiatives and current best practices.

For the DSA, we wish to offer some thoughts and considerations regarding some of the due diligence obligations, which we believe will need to be considered to help deliver a balanced and proportionate framework that addresses stakeholders' concerns.

---

1. On Harmonised Notice and Action Rules

What is a notice?

Online service providers rely on a notice and action regime through which users and stakeholders can submit notices relating to illegal content or activity they encounter on the service (many service providers also employ a separate system for content that is not illegal but violates terms of service, e.g. nudity). The notice and action system is effective but we believe it would benefit from greater clarity and harmonisation, notably on the question of what constitutes a valid notice - in both definition and practice.

DOT Europe questions:

- What do policy makers consider to be a valid notice? A new legal instrument at EU level which defines a notice in an overly broad way, covering any kind of flag or submission by any kind of user without reference to minimum information, will confuse rather than improve service providers' notice and action processes. For example, a "flag" is not the same as a valid notice. Service providers must review and act on the notices they receive on alleged illegalities and to be able to do so they must know what that alleged illegal or violating use is, where it is, and have a reference to the content at issue.
- How will policy makers take account of the variety of notifiers and different actions that can be involved in notice and action procedures? Service providers encounter many different types of notifiers from a variety of authorities and daily users and need some flexibility to be able to react effectively and efficiently.

[1] Formerly EDiMA, see our press release on the launch of DOT Europe here.

DOT Europe recommendations:

- A valid notice should include a minimum series of elements - which ought to also be referenced in the definition of a notice from the outset, to allow for more effective and efficient processing of notices. Such elements should include:
    - A notice made in writing with adequate information on the material alleged to be infringing;
    - An explanation as to why the notifier alleges that the content at issue is illegal, including (where possible) details on the legal ground to demonstrate the unlawful nature of the content in question;
    - The exact location of the material alleged to be infringing e.g. via a URL;
    - A declaration of good faith from the notice provider;
    - In the case of intellectual property rights, identification of ownership with contact details (where possible) and the right infringed.
- A notice must also be submitted to the correct channels to be considered valid, either via an identified email address or another secure method reserved for this purpose by the online service provider.
- Notice and action rules should also take into consideration that notifiers can take many forms, they can come from daily users, rightholders, competent authorities and law enforcement, to name a few examples. Service providers will need to be able to process notices flexibly, depending on the nature of the notifier and the nature of the alleged illegality notified. For example, certain types of illegalities can require a more urgent response (e.g. CSAM, or activity which would give rise to material and bodily harm).
- Action on a notice should not equal content removal per se, rather - as we know the complexity and diversity of cases involved - it is recommended that "action" should take into account any service provider response on the notice, be it via action taken on the content or via updates provided to the notice issuer. Rules should also address the steps that a service provider can take to address notice senders that repeatedly send inaccurate notices or abuse the notice process and allow for fraud prevention.
- Clarity between take-down orders and take-down requests should also be maintained in notice and action rules. Take-down orders are legally binding, whereas a take-down request can be included as a request in a notice, for a service provider to review. In the case of take-down orders, policy-makers should consider how to clarify and harmonise rules on the nature of these orders as well. For example, clarity could be provided as to who can submit a take-down order to a service provider, the scope of the orders, the information to be provided to users following the order, and by which entity – the service provider or the authority issuing the take-down order

2. <u>On Transparency Reporting on Notice and Action</u>

What is meant by transparency reporting?

There is an ongoing debate on the opacity of the notice and action practices service providers have in place, some want more information on the proportion of content that is actually removed from a service versus that which is reinstated for being erroneously removed. Transparency as it is discussed in the context of content moderation and due diligence obligations in the DSA appears to mean different things to different stakeholders.

DOT Europe questions:

- What kind of transparency outputs do policy makers want, and to what end? There seems to be a call for transparency from a variety of angles, without a focus on the kind of outputs that would be helpful to policymakers and other stakeholders. We have seen transparency reporting described as transparency on content policies, transparency on changes to terms of service, transparency of take-down volumes, and transparency on appeal rates - to name a few.

DOT Europe recommendations:

- Given the variety of calls to action, policy-makers should take a problem-specific approach when determining where they would like to see increased transparency and the level of detail required, keeping in mind the possible unintended consequences. For example, there should be a clear distinction made between data that is provided to authorities for enforcement purposes versus data that is aggregated and published for the general public.
- Policy makers also need to determine where there is added value in having such transparency reports outside of what is already being done. The industry is already showing a great deal of transparency with customer facing information on the working of recommendation systems, privacy notices on the use of their data and a number of regular reporting on content moderation etc.
- General reporting requirements are likely to apply better to some services than others, so policy makers should consider how to ensure that any new rules are proportionate. For example, on a live streaming platform the content taken down may be rather low, which is not necessarily an indication of low enforcement but simply the nature of ephemeral type of content. This is similar for a marketplace and a social network – both services are very different, and a reporting framework would have to take this into account.
- Service providers should also be able to contextualise any information they provide. Transparency reporting without context can lead to distorted information which actually runs counter to the purpose of the reporting. An obligation on a service provider to provide detailed reporting on the status of different notices and takedowns can present an inaccurate picture of a situation if the right distinctions are not made in the initial rules. Many complaints received by service providers are inaccurate or abusive, and rules which do not offer a service provider the opportunity to be flexible or contextualise their information may result in a report which presents e.g. a low number of take-downs per notice volume. The use of percentage reporting figures as opposed to absolute figures may also help to contextualise this information.

How often must transparency reports be conducted, and what information is needed?

While there are calls for transparency reporting to form part of the DSA due diligence obligations, the practicalities of this obligation need to be considered.

DOT Europe questions:

- Would transparency reporting have to be conducted on an annual basis, or more frequently? What level of detail would be required per report? At what point is there meaningful transparency compared to a possible saturation of information that cannot be processed? Who are these reports for, do they need a certain level of expertise to understand the information presented?

DOT Europe recommendations:

- Policy makers need to consider who is the target audience of these transparency reports and how they would like to use the information they provide. Working back from this, they can then define how often they need certain information and what purpose it can serve - this will help to define the frequency of reporting and the level of detail required. Transparency in this sense should not be confused with reporting to public authorities.
- Proportionality is key - there is no "one size fits all". Some service providers will have more resources and access to information about the nature of their services than others, this needs to be kept in mind when looking at these rules. For example, regarding the content of any transparency reports, we would advise against the consideration of any horizontal template for transparency reporting across businesses and online service providers - as this will not achieve the desired effect and will not sufficiently take account of the nuances of different service offerings.
- Another point to consider is the idea of due diligence obligations on transparency reporting applying more broadly - for example, by extending the obligation to certain parties submitting notices to online service providers such as rightholders, competent authorities, etc. We believe it would be useful to have more information on where notices are filed, the numbers, the rejection rates and the sort of issues notified (e.g. types of rights, goods and content, infringement in question) - to enhance cooperation among stakeholders and optimise notice and action procedures.

3. <u>On Algorithmic Transparency and Content Curation</u>

What is meant by algorithmic transparency for content recommender systems?

Recent reports from the European Parliament have called for increased algorithmic transparency, especially when it comes to "content curation" on certain services.

DOT Europe questions:

- Do stakeholders mean algorithmic transparency or algorithmic "explainability"? The disclosure of several lines of code detailing the precise functioning of a particular algorithm will not explain to a user why they are seeing a particular piece of content at any given time, but it will likely infringe the IP rights and trade secrets of a service provider. However, explaining how an algorithm learns about a user's interests and preferences can help to educate the user about how services operate so that they can make informed choices and engage with content. Many service providers already provide dashboards tailored to individual users, explaining how the information on a service is offered to them based on their preferences.
- What degree of "explainability" is required? Who is the intended audience for this information and what problem would this obligation try to address? A specific obligation on service providers to publicly report on the details of the functioning of their recommender systems which obliges them to disclose how a certain piece of content can obtain more prevalence on a service can inadvertently provide a guide to bad actors to game these systems, and the virality and spread of illegal content may paradoxically be provoked by such requirements. Furthermore, important legal rights could be infringed, such as trade secrets or intellectual property rights, that would dramatically hinder innovation and competition among online services in Europe.
- How do policy makers envisage that any new rules on this area would interact with transparency rules recently adopted in the P2B regulation and the consumer Omnibus?

DOT Europe recommendations:

- Policy makers will need to consider the granularity of the information required in order to solve the issue without generating broader consequences.
- As it is with transparency reporting on notice and action above, the audience here will also need to be considered. Given the paradoxical risks of providing bad actors with a guide on how to game service providers' systems, we recommend that when it comes to transparency for the general public it should be limited and focus on education and the building of trust among users.

What is meant by content curation?

Some stakeholders have mixed calls for increased algorithmic transparency with calls for service providers to offer users more choice in how they see content on a service, or more control over "content curation".

DOT Europe questions:

- There have been calls for users to be able to "opt out" of content curation, but what does this mean in practice? We would stress that "content curation" can also just refer to content that is organised in a particular way, to make it presentable to a user on an interface. Even a service which organises content chronologically is still technically curating content.
- It will never be possible for a user to completely opt out of how a service provider presents content in some manner or another, in the same way it is not possible for a person going to a supermarket to completely rearrange the shelves there. Many online service providers already offer users options to switch the view of content to chronological order, by the most popular interactions, or by other preferences, in the same way a shopper can choose to walk around a supermarket using whichever route they prefer.

DOT Europe recommendations:

- Policy makers should take account of the fact that content curation can mean the organisation of content in its most basic sense. Calls to offer users complete control of how they see content may be the equivalent of offering users their own APIs per online service, depending on how this obligation progresses in the DSA debates. Practicality needs to be considered here.
- It is critical to determine what the problem is so as to find a proportionate response. The physical world of commerce is "curated" around us, from shops choosing to pay more for a larger frontage in a more prominent part of town to an advert appearing on the inside cover of a magazine. Issues of "amplification" or visibility of similar content that reinforces a particular point of view etc. should not be confused with selection and arrangement across all content in all contexts.

4. On Know Your Business Customer (KYBC)

How can the KYBC principle be made workable for service providers of all sizes?

KYBC is not a new concept but elevating it to a legal obligation in the DSA will require the final rules to be clear, privacy-friendly, and proportionate. They will also need to be supported by the right infrastructure in order to be scalable, while enabling the businesses of all sizes to thrive.

DOT Europe questions:

- How can a smaller service provider successfully contact and onboard all of its individual business users, especially where anyone can create a business page and begin operations?
- The process of screening sellers against publicly available databases for KYBC purposes can be costly and operationally burdensome - how would policy makers maintain proportionality in the application of this obligation? For example, EU VAT and EOIRI numbers can be checked for validity but not for whether the person providing them is the owner.

DOT Europe recommendations:

- To make this proposal workable and proportionate for service providers of all sizes, any verification of business users' identities could be done against publicly available databases. These databases will also need to be both scalable and accessible to avoid blockages. Moreover, verification of data accuracy as collected from users should only be demanded from platforms to the extent that reliable official and updated databases exist and are provided to them by competent authorities.
- Service providers should also be empowered to adopt a risk-based approach to determine any cadence for rescreening of business users.
- Authorities must provide simple and secure ways for service providers to report data, and for their data to be treated following the submission of a report. Transparency or other reporting requirements to authorities can sometimes hinder the quality, relevance, and security of the shared information. Situations can arise in which data structure is not clearly established or even processed by authorities (e.g. systems may fail to absorb high volumes, or to recognize non-Latin characters even when the data is of global nature). The aim should be to adopt standardized technical requirements, whereby service providers are able to automate and ensure the security of the transmission, while retaining flexibility to allow the service provider to develop systems best suited for their services as well.

What is meant by a business customer?

DOT Europe questions:

- Will the meaning of a business customer be defined? Depending on the nature of the service provider, some services will have "official" business users which will be different to business users (i.e. a seller that is not a legal person). Other services such as online file storage, domain provision etc. do not know whether these are being used for business or personal reasons. National laws do not have a neat distinction in place for these concepts, so how will this be reflected in the DSA?

DOT Europe recommendations:

- While no particular technology or method of verification should be mandated here (in order to allow all service providers to adapt to their situation), a publicly accessible database/registry which gathers information on business user information could assist service providers to determine when they are required to gather certain information from specific users.
- Alternatively, a system based on users' self-declaration could be established whereby business users are required to declare their details to a service provider in order for the service provider to then perform their checks based on any KYBC rules.

What is the impact on service providers and business users?

DOT Europe questions:

- The details of the different criteria in a KYBC principle are often discussed, but where will policy makers establish boundaries to avoid unintended consequences for service providers and users in practice?

DOT Europe recommendations:

- A service provider should not be held liable for determining which user is a business by law, they can often only rely on the user's self-declaration as well as any appropriate notice pertaining to the user received in that regard.
- Service providers should not incur liability or be forced to stop providing services to a user based on mere suspicions. The mere fact for a user to provide incomplete or inaccurate data under due diligence requirements does not constitute proof of illegal behavior on the platform, at least until an authority issues a formal notice on the matter.

5. On Notice and Stay-Down

How could a notice and stay-down regime be reconciled with Article 15 of the e-Commerce Directive?

Some stakeholders have called for the introduction of a notice and stay-down obligation for online service providers, to oblige them to keep down content that has been previously notified as infringing activity. Article 15 of the e-Commerce Directive includes a prohibition on imposing a general monitoring obligation on online service providers, meaning that service providers cannot be obliged to generally monitor the information they store nor seek facts or circumstances indicating illegal activity. This protects their users' right to privacy, their freedom of expression and freedom of information, as service providers cannot be obliged to check every user's upload for possible illegalities. Moreover, if a service provider would have to do a blanket monitoring of every user upload, they could be seen to have acquired "knowledge" or "awareness" of an illegality which could lead to the loss of their limited liability protection under the e-Commerce Directive. If this situation were to arise, this would undermine their operation and growth in the Internal Market, as service providers would face possible perpetual liability for every user upload. It would also have an adverse impact on users' freedom of expression and the freedom of information, as service providers would be disincentivised to allow many user uploads on their services, for fear of liability.

DOT Europe questions:

- Some argue that a notice and stay-down obligation would equate to a specific rather than a general monitoring obligation, due to a narrow scope which would only oblige a service provider to check for a specific illegality rather than every possible illegality. The CJEU has indeed imposed specific monitoring obligations on service providers, but with a number of limitations in relation to the nature of the assessment involved, and whether or not such an obligation would result in a monitoring of all users on the service in order to detect a single illegality [2]. Even if a notice and

[2]See for example Cases C-70/10 *Scarlet v Sabam*, C-360/10 *Sabam v Netlog*, and C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland*. Among the limitations placed on specific monitoring obligations, the CJEU has said that said monitoring obligations cannot be "excessive" so as to require the service provider to have to carry out an "independent assessment" of the content, nor can an order consist in the active monitoring of all the users of service in order to identify illegal content, as this would amount to a general monitoring obligation, and that any obligation must be fair, proportionate and not excessively costly for the online intermediary.

stay-down obligation were to only apply to previously notified content, this would still oblige a service provider to check every user upload for the presence of that specifically notified content. Moreover, where it is the use of the content and not the content itself which leads to the alleged illegality, a service provider would be required to make frequent assessments of every use of that piece of content across its service. Is this not in essence a general monitoring obligation?

- How could such any notice and stay-down obligation be made proportionate and workable for service providers of different sizes, dealing with very different types of content and activity? For example, there is a sliding scale between what is identical and similar content, an image can be flipped or edited, while a defamatory statement can be reworded or quoted by another source for reporting purposes. How would any notice and stay down rule be made sufficiently precise so as not to oblige blanket monitoring, but still flexible enough to take account of the many individual decisions that have to be made on the nature and use of any piece of content? Many types of content are not susceptible to such a practice because the content may be illegal at the time, manner and place of the first occurrence but may be legitimate in some other subsequent use – for example because of a license, or fair use in the case of copyright, or because the content describes a product which may have been counterfeit the first time but is being used to describe a genuine item in a subsequent listing.

DOT Europe recommendations:

- Article 15 of the e-Commerce Directive forms an important part of the foundation of rules for online service providers in the Internal Market and ensures the protection of the fundamental rights both users and businesses online. We encourage policy makers to keep the importance of this provision in mind, and consider the relationship between the provisions of the e-Commerce Directive and the aims they set out to achieve – a specific monitoring obligation cannot be employed in either a legal or practical sense as a means of bypassing this rule.
- Policy makers should instead consider how to put safeguards in place in the DSA for service providers to proactively come up with a variety of solutions to address the issues with previously identified infringing content. A legal safeguard which ensures that service providers can take these proactive actions without losing their limited liability protection would avoid this conflict with Article 15 of the e-Commerce Directive.
- Where service providers do voluntarily engage in practices to try to keep previously notified infringing content off their services, it is also important to remember that "keeping down" "identical or equivalent" content is not a static operation. Bad actors will seek to circumvent protections, so there is a continuous process of development that is required to do something effective.

With this paper, DOT Europe aims to raise constructive questions for the ongoing debate on "due diligence obligations" in the DSA. These questions and conversations will likely evolve, but we believe these practical questions need to be a part of these early considerations, in order to achieve a balanced and workable framework for all stakeholders.