Orange position on the future of digital liability

July 2019

The current eCommerce Directive (ECD) has played an important role in the development of the Internet since 2000. Over these two decades, our lives have changed fundamentally in the way we interact, work and organize our lives digitally. For service providers, the current eCommerce framework has been an important tool providing legal assurance. The use of digital services online has also brought challenges. Illegal content can spread online with comparative ease, bringing the need to tackle the issue of harm inflicted on users. In this regard, the focus needs to be on intermediaries that play a direct and active role and economically benefit from the dissemination of such illegal and harmful content and, given such circumstances, should help in meeting these challenges.

We understand that the European Commission is working on a proposal for a potentially new "Digital Services Act". We do not know the exact content of such a proposal and our position is therefore without prejudice to the final proposal, but Orange would like to highlight the following key elements and principles:

1. Maintain the underlying principle of a liability exemption-regime for technical intermediaries, supporting the continuation of blocking on the basis of injunctions where the illegality of content has been confirmed by a judicial authority.
2. Address potential specific problems through targeted interventions focused on where harm actually occurs.
3. Formalize the duty of care related to the removal of illegal and harmful content, targeting it to the sole service providers which allow users to share or discover user-generated content and interact with each other publicly online, and where the service provider has an active role in the presentation of the content.
4. A future "Digital Services Act" should be based on the principle of having harmonised rules across the EU, preferably founded on a regulation.

The new rules that would be developed in the "Digital Service Act" should rely on the existing framework rather than introduce a radically new one

We have as a telco operator the duty and obligation to assure that our customers' personal communications remain confidential. Operators do not have any interest in the content itself of the communication between our customers and customers of other providers of electronic communications services, and we do not benefit in any way from the content exchanged. Our interest is in assuring the availability of the underlying transmission and storage; ensuring that the service is provided and secure. Therefore, the principle of a liability exemption-regime for technical intermediaries should be maintained.

In our role as a responsible provider of traditional telecommunications services, such as fixed and mobile internet access and caching services, and to a growing extent cloud services, we are protecting our customers from illicit communications and illegal content through compliance with requests from judicial

authorities to block access to infringing sites. This form of protection has ensured that only confirmed illegal content has been blocked through injunctions based on judicial review. We therefore support the continuation of blocking on the basis of injunctions where the illegality of content has been confirmed by a judicial authority.

We already apply blocking lists for sites known to promote terrorist content and child sexual abuse material provided by competent authorities, and in addition, we have for many years cooperated with the Internet Watch Foundation to voluntarily deploy their internationally-recognised blocking list to suppress child sexual abuse content. Where possible, we will continue to deploy such measures and contribute to efforts protecting children against child sexual abuse content.

A growing area of commercial interest is in the offering of cloud services. As our lives become ever more digitalized, customers are interested in securing sufficient space to store their own personal and professional content for the future. In this case, the protection of customers' confidentiality must be assured. For instance, businesses should be able to offer secure cloud services, and remain confident that their liability exemption would be maintained where there is no public access to such content, and it is not possible to make a public search of the archives of stored content in order to discover this content.

The definition of the scope should be robust and based on user's harm and thus target relevant actors.

The requirements of increased duties of care should be on providers whose services allow users to share or discover user-generated content and interact with other users publicly online, and as such are characterized by providing access and a possibility to distribute illegal and harmful content to the public. The notion of the particular provider's active involvement in the e.g. tagging, organisation, promotion, optimization, recommendation and curation of such hosted content is an equally important element in determining these providers' ability to identify and remove illegal content. The means to ensure an increased duty of care should especially focus on the protection of users, introducing targeted notice-and-take-down requirements whilst ensuring that a general monitoring of citizens' activities is avoided.

A potential loss of limited liability should continue to be based on the notion of failing to remove illegal content expeditiously upon knowledge or being notified by a competent authority, i.e. a blocking injunction. Due to the differences between services allowing for the availability of content to the public and those protected by confidentiality, notice-and-take-down requests to parties hosting content should be made clearly distinct from blocking injunctions applying to passive providers of access to sites.

Orange believes that conditions related to a category of services on the basis of a large or significant market status is not entirely relevant if related to the removal of illegal content, as the underlying assumption should be that illegal and harmful content should be removed by relevant providers disregarding their number of users. The potential for dissemination of illegal and harmful content is greater the larger the provider, but the potential harm to an individual is the same whatever the size of the company. If the assumption is based on sharing resources such as automated tools for identification of harmful content, this should be determined through voluntary agreements, or through agreed Codes of Conduct.

The concept of "significant market status" raises concerns in terms of definition and interpretation. When looking at existing and robust criteria justifying intervention in a given market, they are based either on

competition law or on criteria mirroring competition law principles (ex-ante rules based on significant market power), which delivers legal certainty and predictability to market players. However, no general regulation of service interoperability is required and any respective revision of the legislative framework should only promote voluntary cross-sectoral projects and standards.

To measure the impact on new initiatives to reduce harm on users, there should be a duty on the European Commission and Member States to observe what effects any extended deployment of measures, including the use of automated tools, to counteract the appearance and removal of illegal content would have on the fundamental rights to freedom to conduct a business and the freedom of expression, and make the results of such observations publicly available.

The proposed piece of legislation should be a Regulation in order to achieve a consistent application across EU

Orange has always been a strong supporter of a digital single market (DSM) and believes that harmonised rules across the EU are critical to achieve such a goal. Therefore, we support the idea that any potential legislative act that would impact the DSM should take the form of a regulation.

Such a new piece of regulation should focus on maintaining a liability-exemption regime, and avoid expanding into areas already covered by other types of legislation, such as the regulation covering end-user rights, platform-to-business, GDPR, or the recently adopted Copyright and Audio-visual Media Service Directives. When infringements occur, a future Digital Services Act should continue to limit itself to establishing the circumstances of when a liability exemption becomes void. This has created legal stability in the past and should continue to provide assurance and guidance.

The choice of having a Regulation as the legal instrument, would not only facilitate an easier implementation of measures, but would also assist SMEs in meeting measures on an equal footing with larger providers. Given that online services are to a great degree pan-European and even global; having fragmented rules would add to the potential harm of European users and be a disincentive for providers to comply. In this regard, we also believe that third country providers targeting a substantial number of European users should be impacted according to the country-of-destination principle as in other consumer protection laws.

Orange does not believe that a new authority is needed. Supervision should be ensured and performed by existing authorities at Member State level, and conflict resolution should be governed by horizontal law. Otherwise, there would be a risk of overlapping competencies that could lead to legal uncertainty. In this regard, any cross-border authority that would like to require a provider to terminate or prevent an infringement should be obliged to file such a request through the competent authority in the Member State where the provider is established. This would allow the latter Member State to determine whether the content in question would be deemed illegal under their national laws and ensure the principle of subsidiarity.

For more information: www.orange.com/committedtoeurope or follow us on Twitter: @Orange_Brussels