DIGITALEUROPE

DIGITALEUROPE Position Paper on the proposed Regulation on 'Preventing the Dissemination of Terrorist Content Online'

Brussels, 21 November 2018

DIGITALEUROPE's membership fully supports the efforts of the European Commission to fight terrorism and incitement to violence. We believe this is a key policy area that, if done right, will help reduce the dissemination of terrorist content online.

Our member companies have undertaken extensive work to fight terrorism and incitement to violence, including expanding their cooperation with law enforcement authorities and increasing available measures to tackle extremist content on a voluntary basis.

It is important that policymakers carefully consider the issues at stake, most importantly, aspects regarding rule of law, fundamental rights, and the feasibility of implementation for hosting service providers. Finding the right approach is not easy, and it is crucial to bear in mind that this Regulation will also further define how we generally consider duty of care of platforms. Moreover, the Regulation could have knock-on effects for innovation and the future of internet services.

The proposed measures need to be consistent with the long-established e-Commerce Directive by ensuring that they are appropriate to the technical and organizational nature of the online world and providing legal certainty for the covered hosting service providers.

We agree with the Commission that it is important to uphold the current legal framework as set out in the e-Commerce Directive, and whilst we understand the urgency of the drive to tackle terrorist content online, it is crucial that this Regulation is workable and properly considers the unintended consequences on the broader digital economy. Specifically we believe that the current legal framework as set out in the e-Commerce Directive must not be undermined or derogated from.

1. A clear scope that is fit for purpose

The scope of the Regulation in its current form potentially sweeps in many services on which terrorist content is rarely a problem. The proposed definition is too broad and unclear, and risks capturing a significantly larger than intended group of information society services.

The Regulation does not differentiate, for example, between services whose primary purpose is to make content widely available to the public by default and those that are used primarily for personal storage of private content and are not designed to facilitate broad dissemination of content. As such, companies will struggle to understand which services are captured in the proposal.

We urge the co-legislators to clarify the scope and specify which types of services are covered by the regime. The legal uncertainty and ambiguity is unjustified, given the high sanctions and significant investment required to devise measures and procedures to comply with obligations foreseen in the Regulation, even in an environment that does not pose a risk for the dissemination of terrorist content. According to the European Commission's own impact assessment, the Regulation would cover 10,500 hosting service providers established in Europe. However, Europol reports that only 150 companies[1] were identified as hosting terrorist content, a large part of them being established outside of Europe and offering their services across the Single Market.

The scope of the proposed Regulation should be narrowed to providers that enable its users to make content available to the general public. This would limit the unintended consequence of covering services that are not the target of the Regulation.

a) Limit the scope to services that publicly share content

The Regulation is concerned with terrorists reaching large undefined audiences for purposes such as grooming, recruitment and glorification of their atrocities. Enterprise and cloud services which allow users to share content with selected users (but not with the general public) do not serve this purpose, as they are used primarily for collaboration between colleagues or sharing photographs or documents between small groups of family and friends. There is a significant difference between the reasonable expectations of privacy of a user who shares something in a medium that can be accessed by anyone and that of a user sharing material with a limited group of individuals in a closed end-user group. By limiting the scope to those services that make content generally available to the public, a balance between privacy and security can be found. This also aligns with the Directive on Combating Terrorism[2] that refers to the dissemination of content to the public.

We therefore urge the co-legislators to narrow the scope of the Regulation to hosting service providers that enable their users to make content available to the general public.

b) Exclude cloud infrastructure service providers

Cloud infrastructure service providers are often referred to as the 'building blocks' for digitalisation and IT, acting as an initial layer of foundational infrastructure and enabling customers to build and run their own cloud-based IT systems which are designed, controlled and managed by the customer.

For instance, a cloud infrastructure service provider, by definition, cannot have knowledge of the content or the data that are stored in its infrastructure and has no technical tools available to monitor such content or data. A cloud infrastructure service provider does not always have a direct relationship with the user uploading the alleged terrorist content and does not control the data that is made public.

[1] Impact assessment: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017L0541

The technical feasibility of compliance without causing wider negative impacts on core operations remains doubtful because cloud providers are often not technically capable of blocking specific content. Even if cloud service providers wanted or were requested to remove or disable access to specific content, this would require them in many cases to block or remove lawful content from thousands of users. Blocking individual alleged illegal content would force cloud infrastructure providers to take down entire services. For instance, if a comment made in a blog were considered terrorist content, cloud infrastructure service providers would in most instances only be able to take down the entire website or blog.

For all of these reasons, we urge the co-legislators to clarify that the Regulation does not apply to cloud services that purely provide the backend infrastructure and do not share content to the general public.

2. A workable deadline for hosting service providers

The one-hour deadline for content removal does not take into account several practical difficulties such as the need to translate the request, the need to identify whether the request came from a valid competent authority, the technical operations to remove the content, the international dimension of the internal organization of several hosting companies, and even time zone differences.

Small and medium-sized providers especially lack adequate compliance resources. This requirement would force over 9700 SMEs established in Europe to hire an average of 15 persons per company all around the clock just to monitor (potential) requests.

The tight deadline, in combination with the broad definition of terrorist content, the very broad interpretation of competent authorities and the absence of any redress option for users (aside from going to the national competent authority issuing the request) creates a worrying situation that could be open to abuse and provides insufficient protection for fundamental rights.

The Regulation itself (Art 4.6) refers to the notion of 'without undue delay' in other instances, which is a common practice in EU legislation[3] and is present in several Member states' national law.[4] Companies of all sizes need the time and opportunity to take appropriate and balanced action against their end-user and minimize collateral impact.

Accordingly, the timeline for hosting service providers to comply should be 'without undue delay' from receipt of the order, allowing service providers sufficient time to address each request.

[3] General Data Protection Regulation (art 33.2)

[4] For example, under French criminal code, the Prosecutor or police officers may request the communication of any piece of evidence related to an investigation that is stored in the companies or public administrations' the IT systems. The said companies or administrations must provide the requested evidence without undue delay (art. 60-1 CPP).

3. A clearer definition of terrorist content

The recitals to the Regulation rightly identify that terrorist content can be legally disseminated for many valid reasons including educational, journalistic or research purposes and that radical, polemic or controversial views should not be considered terrorist content. For material hosted on cloud service providers, where broader context is unavailable, it is frequently impossible for providers or authorities to make such distinctions.

Some types of content can be easily identified as illegal, while other content such as speeches require nuanced judgment. Moreover, there needs to be more certainty around the definition of terrorist organizations. Greater clarity is possible by limiting the definition of terrorist organization to those on the EU or UN designated terrorist organizations lists.

The definition of 'terrorist content' should be clarified and linked to a designated list of terrorist organisations in order for companies to be able to create a more manageable process. We also recommend that the Recital 9 language setting various legitimate forms of expression be included in the main text of the definition.

4. Proactive monitoring obligations jeopardizing the e-Commerce Directive (ECD)

a) Continued use of the voluntary framework

DIGITALEUROPE's member companies have invested in developing technology to combat and counter terrorist propaganda. We would call for this voluntary regime to be maintained alongside the Regulation since it has been working well. Legal protection is needed for platforms and providers who take proactive measures to take down harmful content, and it should be clarified that by doing so they would not lose liability protections.

It is unclear to companies how the proposed Regulation affects the relationship between private terms of use and regulatory obligations, and what the impact is on the rule of law. Given the broad scope of the Regulation and the potentially highly intrusive nature of proactive measures, it is also essential that there be an independent arbiter that can assess whether the right balance has been struck — i.e. that considers the impact of the measure in limiting access to online terrorist content against its impact on the rights of the provider and its users. To address this issue, we recommend that Article 6 be amended to give hosting service providers an express right to appeal to national courts any decisions by competent authorities requiring hosting service providers to implement proactive measures.

b) Compatibility of the proposal and the e- Commerce Directive.

As it stands, the Regulation departs from the principles of limited liability as established in the e-Commerce Directive. Undermining the regime of Directive 2000/31/EC will have far-reaching consequences for start-up businesses in Europe, for users and for fundamental freedoms creating a slippery slope. We believe that this may have consequences for other types of illegal content, and safe harbour considerations.

Existing European law does not allow Member States to impose a general obligation on hosting service providers to monitor the information that users transmit or store. However, in the proposal the Commission argues that, given the 'grave risks associated with the dissemination of terrorist content', states could be allowed to 'exceptionally derogate from this principle under an EU framework'. This exception could clash with other fundamental rights including citizens' right to privacy and free expression.

We therefore urge co-legislators, before moving forward, to conduct a proper legal analysis on the compatibility of the proposal and the e-Commerce Directive[5] to the extent hosting service providers follow their obligations under the Regulation and are exposed to removal of lawful content or privacy violations. This Regulation should not adversely affect the application of Article 14 of the e-Commerce Directive. To undermine the regime of e-Commerce Directive will have far-reaching consequences for start-up businesses in Europe, users and for fundamental freedoms. It is critical that the current regime is upheld in this Regulation and new safe harbours are introduced.

c) The impracticability of compliance with general monitoring obligations

Millions of terabytes of data are stored, accessed and exchanged online between businesses and customers. Any proactive monitoring obligations must take into account the state of technological development and feasibility of such measures for companies, who are better placed to assess those measures. Companies are the only ones holding the necessary expertise on tools and technical processes to decide on the duty of care and proactive measures to fight terrorist content online effectively. On top of that, it is not feasible for companies to develop specific national technological solutions for each country. It risks even leading to censorship and fragmentation.

The application of proactive measures to non-public material such as content shared privately via cloud amongst groups of friends, family or colleagues would have even greater implications for fundamental freedoms and cybersecurity. It could violate users' fundamental right to privacy and undermine their reasonable expectations of how their content is safeguarded.

Additionally, in many cases hosting service providers may not have access to their customers' data and may therefore not be able to scan or filter all the content that is being processed since they do not control or have access to the data, which in many cases is encrypted. This applies to enterprise services as well as cloud infrastructure service providers. In addition to technical limitations, a general monitoring obligation would violate the commercial and privacy interests of users.

The Regulation envisages a patchwork of different requirements on the imposition of proactive measures that vary based upon which competent authority is responsible, country of jurisdiction and whether or not they have rendered a decision on a specific provider at a given moment in time. The threshold for having such measures applied is low – one removal order (one piece of content that may or may not be proven to be illegal) can trigger this.

[5] Art.15 of the e-Commerce Directive.

5. A data disclosure obligation that is workable

Service providers will be obliged to keep a copy of all the alleged terrorist content that they have pro-actively removed for 6 months, with possible extension. We seek to understand the Regulation's connection with existing European jurisprudence[6] to ensure the proportionality and consistency of data preservation. Hosting service providers should not have the burden to preserve the content and related data for an unlimited period of time, simply because an authority may need it. This obligation could be limited to a six-month period, specifying that the content and related data may be transferred at the request of the competent authority. Preservation of data should be limited to removal orders as opposed to referral orders, upon request.

We also warn against the excessive requirements to proactively disclose information to authorities. As written, this obligation could result in significant over-reporting by hosting service providers. It could also stifle online speech by parties concerned that their expression might be misreported as evidence of a terrorist threat. Any disclosure of content-related information should follow due process in line with the e-Evidence proposal, and not leave providers in a complicated position to assess whether or not content is considered a threat. If this reporting obligation is retained in the Regulation, it should be significantly narrowed so that it applies only in exceptional circumstances, where the available evidence demonstrates a clear risk if imminent harm.

6. A single judicial authority per Member State

The Regulation states that a removal order can be issued as an administrative, judicial or law enforcement decision by a national competent authority. The process to identify such competent authorities is not detailed in the proposal. Since the measures pronounced by the 'competent authority' have to strike the right balance between several potentially conflicting rights, the intervention of a judge is necessary and represents an additional safeguard.

DIGITALEUROPE's membership is concerned that an administrative body may not have the expertise to issue a valid order that is proportionate to the threat, respects fundamental rights and avoids the erroneous removal of legal content. Having multiple authorities will make it more difficult for companies to evaluate and reply in a timely manner because they will need to apply high judgement as to the adequacy of the request and evaluation of the material.

Therefore, it is crucial that each Member State should have a single judicial authority that notifies the hosting service provider that content must be removed. A single point of contact (SPOC) system has proven to work very well in Member States that have put it in place for law enforcement data access requests. It makes the system far more efficient, as it decreases the turnaround times to process requests, facilitates cooperation with service providers and provides more legal certainty.

[6] Tele2 Sverige AB (C-203/15)

7. Grounds for challenging removal orders and a due process

We believe there is a risk that removal orders could be misused in ways that pose a potential threat to EU fundamental rights. As currently drafted, a removal order becomes final when it has not been appealed within the deadline, according to the applicable national law of the competent authority issuing the removal order or where it has been sustained following an appeal.

For instance, this would mean that companies would have to challenge a request made by the Romanian competent authority under Romanian National Law which is extremely burdensome since it would entail hiring a local law firm in case the company does not have the resources in that country to challenge the request. Competent authorities already mistakenly send reports on material that is legal and not harmful in any way. The Regulation does not include any safeguard or redress option for companies in these situations other than taking this to court or to the administrative body, which is unbalanced.

We aim at including a clear and due process in the Regulation, including appropriate safeguards, to comply with and challenge orders.

8. Referrals that preserve the liability exemption for hosting service providers.

The envisaged referral system raises a number of concerns. Whilst service providers will enforce their terms and conditions, the Regulation essentially privatises the assessment of terrorist content. It should be clear that, where the competent authority chooses to address a referral rather than a removal order to the hosting service provider, any decision taken by the provider pursuant to the referral should not result in a breach of its duty of care under Article 3, nor in losing the benefit of the liability exemption provided for under the e-Commerce Directive, in line with the Good Samaritan principle. In addition, a more clearly defined role for Europol as the hub to direct all referrals to companies would create a more efficient streamlined process that reduces error and duplication.

9. Transparency reports that are limited to the necessary information

The content of the annual transparency reports should be limited to the information that is necessary to comply with the objective, as identified in the Impact Assessment (page 22), of ensuring that *"citizens, and in particular Internet users, and public authorities have sufficient information to appraise the actions taken […] to detect, identify and remove illegal content"*. It is important that the transparency report exclude unnecessary or confidential information, including information that would be counterproductive and can be used by terrorist organizations or other organizations to circumvent the measures.

10. Sanctions would trigger overbroad deletion of content

The sanctions proposed in the Regulation would create the wrong incentives for companies to overly block and remove content.

Moreover, it lacks the fairness of a sliding scale – in other words, a lower percentage for first infractions that increases with each subsequent violation. On top of that, the fines would lead to a dangerous fragmentation, with different rules in each country, and no real safeguards specifying how and when they would be applied. We welcome a clearer definition of a systematic violation.

11. Conclusion

We urge the Commission to conduct a proper impact assessment on the different businesses and services captured in the Regulation. Further, we aim to see workable rules for companies to be able to comply without disrupting their business models, with due process and with appropriate safeguards, for companies to be able to challenge orders.

We stand ready to cooperate with co-legislators to improve the current proposal to create workable and clear rules for companies.

For more information please contact:
Jochen Mistiaen, Senior Policy Manager
+32 496 20 54 11 or jochen.mistiaen@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total over 35,000 ICT Companies in Europe represented by 63 Corporate Members and 39 National Trade Associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK