Brussels, December 2018

BSA | The Software Alliance's position paper on the draft EU Regulation on Preventing the Dissemination of Terrorist Content Online

BSA | The Software Alliance ("BSA"),[1] the leading advocate for the global software industry, welcomes the opportunity to provide its views to the European Commission's proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online ("Terrorist Content Regulation"). Our members support the efforts of the EU institutions to tackle illegal content online. We recognise that online platforms have important responsibilities to improve the effectiveness of the fight against terrorist content online and we share the desire of the European Commission to ensure that terrorist content online is removed in a timely manner which provides legal certainty for service provides and citizens.

We are concerned that the draft Regulation has chosen to tackle the issue of terrorist content online with a "one-size-fits-all" model. Such an approach fails to adequately take account of the fact that different types of services merit different rules. A future EU framework centered around a horizontal approach to the removal of terrorist content online risks negatively impacting the European enterprise cloud economy. As a consequence, we encourage the co-legislators to focus their attention throughout the legislative process on differentiating between various types of hosting service providers so that the draft Regulation properly takes into consideration the different risk profiles provided by enterprise-based cloud computing services. More specifically we would like to bring to your attention the following issue-specific points:

Issues and BSA Positions

1. Definition of Hosting Service Providers ("HSPs")

The draft Regulation applies to HSPs (Article 2(1)) without drawing *any* distinction between the existence of different types of service providers in today's marketplace. The definition proposed by the European Commission's draft legislative proposal covers a vast array of services that store content uploaded by their

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.*

BSA's members include: Adobe, Akamai, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

users, despite many such services serving vastly different purposes for their end-users (consumers and enterprises). This broad definition would include cloud services, E-mail services, social media, app-stores, instant messenger services, web-hosting services, professional networks, news websites with comment functions and software development services. These services raise significantly different risk profiles with regard to the dissemination of terrorist content online, yet this is not properly reflected in the obligations and measures imposed on service providers by the draft Regulation, particularly regarding the business-to-business services and/or private cloud storage services.

2. Making Content Available to "Third Parties"

We are particularly concerned about the reference in Article 2(1) of the draft Regulation to HSPs making content available to "third parties." By referencing content made available to "third parties" rather than content made available to "the public", the draft Regulation suggests that a wide range of providers will be caught by the scope, including all cloud infrastructure providers. Providers offering enterprise cloud services are not used to disseminate content to the public and as a consequence these services raise significantly different risk profiles with regard to the dissemination of terrorist content. We firmly believe that such services should not be the intended target of the future legislative framework.

3. Criteria for Excluding Providers of Business-to-Business HSPs

The future legal framework should be tailored and limited in scope to avoid capturing all types of HSPs irrespective of how they function or how they are used. Such an approach would allow for competent authorities to focus on those services where the dissemination of terrorist content represents a **true** threat to society**,** while simultaneously avoiding placing burdensome costs on business-to-business software entities. To ensure that the proposed draft Regulation creates an effective set of rules that are necessary, proportionate, and in full respect of European fundamental rights, the scope of the draft Regulation should exclude providers of business-to-business hosting services for four central reasons:

- **Technical Limitations:** Enterprise cloud providers are not in a position to identify which of their cloud customer's users is associated with objectionable content posted online. Consequently, a enterprise cloud service provider would have no other option than to shut down the entire service of the customer. The particularity of these services is that only the cloud customers have absolute control and responsibility over their own data and the services that they operate, unlike with social media platforms, video streaming services, video, image and audio sharing services or file sharing mentioned in Recital 10. As a result, an enterprise cloud 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.

- **Data Access:** Enterprise cloud providers do not have unfettered access to the data stored in their cloud infrastructure by enterprise customers in a way which would allow them to monitor or filter illegal content and control the data that may be made public. Complying technically with this draft Regulation without causing wider negative impacts on core operations remains questionable as enterprise cloud providers are frequently not technically capable of blocking individual alleged illegal content. Blocking and removing specific content would in many cases require to take down entire services.

- **Risk Assessment:** It is important to indicate that the action of disseminating terrorist content online is strongly linked with making some content available to the public. This Regulation does not differentiate between services whose primary purpose is to make content widely available to the public and those that are used primarily for business-to-business purposes and are not designed to facilitate broad dissemination of content. As the content stored by business-to-business HSPs is often not accessible to the public, there is limited risk of wide-spread dissemination of terrorist content online, making it unnecessary for such service providers to set up the infrastructure and monitoring obligations required by this draft Regulation. The essence of this Regulation is to ensure that terrorists cannot reach large undefined audiences for purposes such as grooming, recruiting, preparing attacks, calling for attacks or glorifying their atrocities. There is a distinctive difference between 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. Enterprise cloud providers allow sharing content with selected customers but not with the general public. Imposing the Regulation's obligations onto enterprise cloud services is therefore unnecessary and disproportionate.

- **Privacy Considerations:** Enterprise cloud providers are often not technically capable of applying such filtering technologies nor are they in a position to systematically review content from their customers. This would possibly require them to go against terms and conditions of their contracts and oblige them to filter, for example, personal, corporate, medical or financial data of millions of persons, businesses or governments. In order to ensure privacy and data protection for their customers, enterprise cloud providers do not review content that may be stored in their system. The right to privacy and data protection thus must be carefully balanced against the danger of dissemination of terrorist content online. It is important for the majority of users to protect the right to privacy when sharing material on a cloud service, particularly for those services which are designed to have limited or no access for the public. Imposing obligatory "automated proactive measures" to monitor data storage taking place on enterprise cloud services in Europe should be avoided.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

4. Recommendations

For all the reasons set out above, we urge the co-legislators to narrow the scope of the draft Regulation to HSPs that enable their users to *make content available to the general public*. Furthermore, a specific reference should be made in this draft Regulation to *exclude enterprise cloud services* that purely provide business-to-business cloud services, do not share content to the general public and have no general control of and access to the content of their customers' data.

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315