IMPACT ASSESSMENT ON ILLEGAL CONTENT ONLINE
STAKEHOLDER CONSULTATION:
MEMBER STATES

Introduction:

Following the initial discussion with Member States at the EU Internet Forum (EUIF), the Commission would like to get more detailed views on possible actions to more effectively tackle terrorist content online as part of the ongoing work on the Impact Assessment on Illegal Content Online. These views will complement the Open Public Consultation (OPC, available here), as well as the data collection exercise based on the table of indicators.

The Commission started work on an impact assessment outlining potential problems, objectives and options in the attached Inception Impact Assessment (IIA). As part of the options to be considered, the Commission will analyse the current situation (baseline scenario) as well as actions to reinforce the voluntary measures as well as possible sector-specific legislation (including in particular on terrorism content online) as well as horizontal legislation applicable to all types of illegal content.

The measures presented in the Inception Impact Assessment[1]are initial ideas, and additional actions and options could be considered. The actions to be undertaken would be mainly addressed to online platforms, but could also require further action by Member States.

Member States are kindly requested **to reply to the questions below and provide any additional considerations in writing by 13 June 2018**. The results of this questionnaire will be presented and discussed at the **forthcoming meeting on 15 June**. In parallel, the European Commission's Directorate-General for Communications Networks, Content and Technology convened its expert group under the eCommerce Directive also feeding into the work of the impact assessment.

[1] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1183598_en

Questions

I. Problem and baseline scenario

1. What are the **provisions, arrangements etc. under national law addressing the removal of terrorist content[2] for preventive purposes** (e.g. do you have duty of care provisions[3], specific notice and action procedures, provisions on transparency of companies' actions in relation to the removal of terrorist content, provisions on safeguards, etc.)? Please indicate below – where relevant – the applicable laws or other legal documents.

Notice and action procedures	Law 43/2015 provides for the removal of on line illegal contents by service providers at the request of Judicial Authority offences covered by articles 270 *bis* and 270 *sexies* of the Italian penal code (Conspiracy to commit a terrorist act). In case of contents hosted on servers provided by third parties, only illicit contents shall be removed, without prejudice to the entire web space. Service Providers have the obligation to comply with the judicial request within 48 hours of receiving notification. In case of non-compliance, the Judicial Authority may order a preventive seizure of the internet domain, banning the related access.
Transparency rules	
Safeguards	

Do you have **specialised entities that notify/refer terrorist content** to hosting service providers? What is the **legal basis and benchmark for notification/referral** (illegality of content, terms of service of hosting service provider)?

The provision stipulates that the removal request made by order of the Judicial Authority is forwarded to the hosting service provider by the Postal and Communication Police Service. As above mentioned, the legal basis and benchmark for notification/referral are both illegality of content and terms of service of hosting service provider.

Do you consider them **sufficient** in terms of preventing accessibility of terrorist content? What are the limitations?

Yes, we do.

[2] For the purpose of this questionnaire, "terrorist content" is defined as in the Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final). https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[3] See recital 48 of the Directive on electronic commerce https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031

2. Do you consider that the **amount of terrorist content online** in the last [two] years has overall

	Decreased substantially
X	Decreased
	Continued at the same level
	Increased
	Increased substantially

Please indicate the basis for your assessment. What do you think has contributed to this trend?

The fact that the main online platforms have intensified their self-regulatory efforts to better detect, identify and remove illegal contents, also through cooperation with authorities. Progress in speed of removal has also contributed to this trend.

Furthermore, as emerged from operational analysis carried out on daily basis, the loss of Caliphate lands produced a decrease in the production and distribution of illegal contents, probably because the IS is now reorganizing itself.

3. Do you see a **risk that removal by companies** on their own initiative could **interfere with investigations or intelligence gathering**? What would be the **mitigating measures** necessary to address any such risks?

Due to companies remove contents without noticing Law Enforcement, let alone providing computer data concerning the contents removed, we consider that could be a significant risk. Actually, in this way, any ongoing investigations may be compromised.

It would be useful if Industry stored digital data concerning the contents removed and gave notice to Law Enforcement, in order to allow every possible investigation or follow-up aimed to track those responsible.

4. Do you see a risk of **erroneous removal** by platforms of legal content (e.g. removal of content misidentified as illegal, removal of content disseminated for research, educational or journalistic purposes, "over-removal")? Are you aware of **any cases** of over-removal? What would be the **mitigating measures** necessary to address any such risks?

We don’t have any information in this field.

Non regulatory options: reinforcing voluntary action

1. Do you think that the work under the **EUIF** as reinforced and complemented by the **Recommendation** is **sufficient** action at EU level to effectively tackle terrorist content online?

From the Italian side, we consider that proactive cooperation between private sector and Law Enforcement carried out within EUIF, allowed to establish a solid basis in order to tackle and prevent terrorist contents on line spreading.

2. Do you consider that the **EUIF's work should be further developed** in order to reinforce action at EU level to tackle terrorist content online e.g. through a Memorandum of Understanding in which companies and possibly Member States would sign up to concrete commitments (see possible measures below)?

In our opinion, EUIF should continue along the same line of the progress made so far. However, it could be useful an increased involvement of the companies; a continued confrontation and a solid boost to the development of new technologies. It does not appear necessary to adopt a formal instrument.

3. Which of the following **possible elements** should in your view be addressed and further developed within a voluntary approach? Please indicate the need from a scale from 1 (unnecessary) to 5 (very necessary)

3	More specific objectives for companies' actions (e.g. request a certain percentage of content taken down within a certain time limit)
3	Stronger commitments in terms of internal processes and resource allocation (e.g. to have certain procedures in place, conduct risk assessments and establish mitigating procedures, content of Terms of Service, training, capacity to detect content in different languages)
5	Standardised working arrangements between companies, law enforcement and Europol to enhance understanding of how platforms are abused, to improve referral mechanism, avoiding unnecessary duplication of efforts, facilitating requests from law enforcement agencies in relation to criminal investigations[4].
4	Stronger commitment on specific proactive and preventive measures (i.e. further development and participation in industry-led schemes, such as the database of hashes developed in the context of the EUIF)
2	More detailed requirements on transparency and reporting
1	More detailed requirements to companies on safeguards against over-removal
2	Establishment of an external audit/monitoring mechanism
5	Establishment of contact points, both in companies and Member States, to facilitate referrals (and feedback) and requests from law enforcement authorities in relation to criminal investigations.
1	Additional support (e.g. by Europol) to referral capacities in Member States

[4] See point 40 of the Recommendation.

4. What other additional measures could be developed within a reinforced voluntary approach?

It would be useful if companies reported to Member States when a content is specifically linked to their territories and provided, in addiction, related digital data.

5. Which further actions could be taken to secure participation from those **companies** who have **not engaged**?

As confirmed by the last results regarding the involvement of new Internet Service Providers within the EUIF, it is needed to improve this activity addressing our efforts towards private stakeholders who have not engaged yet, also through the cooperation of the main web companies.

6. Which further actions could be taken to **support small companies** and start-ups in tackling terrorist content online effectively? Should these be taken by larger companies, public authorities or both?

We consider essential the role of larger companies, in terms of assistance, training and providing technical tools in order to automatically detect and remove illegal contents.

7. Do you think that the voluntary approach is **effective** and flexible enough to ensure that companies continue their efforts in the **long term**? Please indicate with which statement you would agree with:

X	Yes
	No, it should be reinforced as presented above to obtain sufficient guarantees
	No, it should be reinforced via legislation

II. Legislative options

1. Why would you consider **legislation necessary at this time**? What would be the concrete benefits? What **risks** could legislation entail?

Thanks to the great results achieved through the voluntary approach, at this time, legislation measures might not be necessary. Indeed, before creating a European Law in this area, it should be useful identifying properly the consistency of regulatory action compared to the objective to achieve. As a matter of fact, in this context, the competence of Member States and European Institutions collides with the reality of companies, who, for the most part, don't have their legal domicile in Europe. The voluntary compliance of web Industry, instead, allowed us to overcome in part these limits.

2. What should be the **material scope of legislation** (i.e. how should terrorist content be defined)? Do you consider that covering material inciting to commit terrorist acts

(Article 21/Article 5 of the Terrorism Directive[5]) is sufficient or should the dissemination of material pursuing other terrorist purposes be included as well?

Material the dissemination of which pursues the following objectives should be included in legislative measures:

X	Recruitment for terrorism
X	Providing training for terrorism
X	Terrorist financing
X	Other, please elaborate: On line self-radicalization

To what extent should material produced by UN/EU designated terrorist organisations be included?

Within a legislative framework, it could be not mandatory to include the source of the material to define it as terrorist content. Otherwise, mentioning specifically UN/EU designated terrorist organisations, it might be a possible solution.

3. Which **measures** (based in particular on the elements mentioned in the Inception Impact Assessment) do you consider as **necessary elements of legislation** to be impactful? Please indicate the need from a scale from 1 (unnecessary) to 5 (very necessary)

2	Definition of terrorist content (*see question above*)
1	Requirements regarding the companies' terms of service
4	General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)
4	Specific requirements in terms of action upon referral (including time limit of one hour)
4	More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)
2	Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms
5	Sanctions in case of non-compliance
5	Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material
1	Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)
4	Requirement to Member States to increase referral capabilities, quality criteria for referrals and for referral entities in Member States to provide relevant support to companies in case of doubt about qualification as terrorist content (e.g. through points of contact)
5	Nomination of point of contact within Companies
4	Reporting obligations for companies[6]

[5] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541

2	Transparency requirements for companies vis a vis their users[7]
3	Compulsory safeguards, such as the ones in the general chapter of the Recommendation
1	The establishment of an external audit/monitoring mechanism for assessing compliance of companies.

Do you consider that minimum requirements could usefully be complemented by self-regulatory measures? And if so, which ones?

- Transparency requirements for companies *vis à vis* their users.
- Requirements regarding the companies' terms of service.
- Nomination of point of contact within Companies.
- Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material.
- General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content.
- Reporting obligations for companies.
- Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms.
- More explicit and detailed obligations to deploy specific proactive measures (including automatic detection).
- Specific requirements in terms of action upon referral (including time limit of one hour).

4. What **other additional measures** could be developed within legislation?

/

5. What should be the **personal scope of the legislation**? Only hosting service providers within the meaning of the Directive on electronic commerce or other service providers?

/

Do you think **smaller companies** should be covered by all obligations or should they be exempted from some of the obligations (e.g. proactive measures) but obliged by others (e.g. time-limits after referral)? Which companies could be partially exempted and from which obligations?

/

6. How do you see the **impact on fundamental rights** of the above-mentioned measures and which safeguards would be necessary to avoid undue interference with fundamental rights?

We don't have any information in this field.

[6] See point 41 of the Recommendation.
[7] See points 16 and 17 of the Recommendation.