

This document has not been adopted or endorsed by the European Commission. Any possible measures indicated in this paper are the preliminary elements being considered by the Commission services, they do not preclude the measures to be finally considered in the Impact Assessment and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the Member State or entity to which it is addressed for discussions and for the preparation of the Impact assessment and may contain confidential and/or privileged material.

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 Assessment¹ 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.

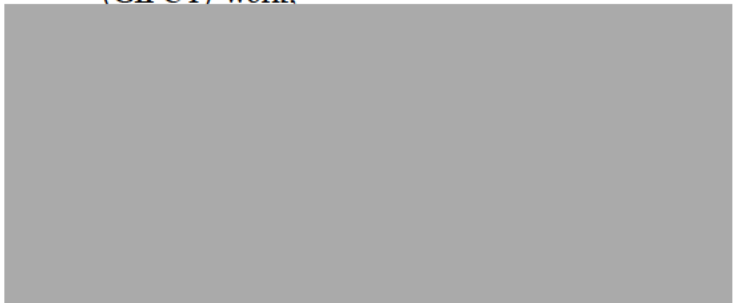
Member States are kindly requested **to reply to the questions below and provide any additional considerations in writing by 13 June 2018**. The results of this questionnaire will be presented and discussed at the **forthcoming meeting on 15 June**. In parallel, the European Commission's Directorate-General 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 content² for preventive purposes** (e.g. do you have duty of care provisions³, 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	<p>Industry cooperation for notice and action operates on the basis of voluntary arrangements between the Metropolitan Police Service's Counter Terrorism Internet Referral Unit (CTIRU) and industry.</p> <p>While there is provision in UK law for the police to issue a notice and takedown order where unlawful content is hosted in the UK, CTIRU instead refers content that breaches TACT (Terrorism Act 2006) legislation to companies for removal on a voluntary basis. If companies agree that the content breaches their terms of use they remove it.</p>
Transparency rules	<p>Industry transparency data is currently made available on a voluntary basis via the EUIF process and companies' own reports.</p> <p>Action being taken to improve the breadth of metrics and usefulness of transparency data via the:</p> <ul style="list-style-type: none">- EUIF process;- Global Internet Forum to Counter Terrorism's (GIFCT) work; 

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>

Safeguards	<p>Companies remove content on a voluntary basis according to their own terms and conditions or community guidelines.</p> <p>Some companies have their own safeguards – including human reviewers – in place to ensure only content that breaches their terms of use is removed.</p> <p>Some companies also have processes in place to review whether content that has been removed, should have been removed e.g. dip sampling.</p>
------------	--

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 CTIRU unit only refers content that is thought to breach TACT (Terrorism Act 2006) legislation.

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

No. Although referrals from users and entities such as CTIRU have an important role to play it is done on a case by case basis and is very time consuming.

We consider that referrals are too slow in reacting to the threat and cannot cope with the range of volume of content.

Speed of dissemination is increasingly important: our research shows that approximately a third of all links to Daesh propaganda are disseminated within an hour of release. Online terrorist content could be ‘live’ for hours or even days before it is referred to a company for removal.

If there are multiple pieces of the same terrorist content on a site (e.g. on YouTube, Google Drive and Google+), the CTIRU have to make individual referral requests for each individual URL to ensure companies take action across all their platforms.

One example of referrals' limitation can be seen in Twitter's most recent transparency report, which showed that only 0.2% of suspended accounts were manually referred by government. The vast majority was identified and suspended by Twitter's automated technology, including 74% before tweeting even once.

Referrals, by their nature, are unable to prevent identified terrorist accounts or content reaching the public.

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 above answer and below commentary is specifically about Daesh content.

It is a due to a combination of factors:

Large companies are responding to the threat, decreasing the overall volume of material online. The EUIF and international community has put pressure on the major companies to expand the use of automated removals and they have announced the following statistics in their recent transparency reports:

- As of December 2017, Google announced that 98% of the videos removed for violent extremism were identified by machine learning algorithms.
- Facebook announced that it had taken action on 1.9 million pieces of Daesh and al-Qaeda content in Q1 of 2018 – about twice as much from the previous quarter. 99% of this 1.9 million was not user reported, but found through FB technology or internal reviewers.

- Twitter also announced in April that, between July and December 2017, 274,460 accounts were suspended for violations related to promotion of terrorism, and of those suspensions 93% consisted of accounts flagged by internal, proprietary spam-fighting tools, while 74% of those accounts were suspended before their first tweet.
- There is still more to be done in engaging smaller platforms, but we have made a good start.

In addition, the military campaign against Daesh has brought down the level of production of official propaganda from its peak.

However, a smaller volume of content, much of which is recycled, or unofficial supporter created content, is now dispersed across a greater number of platforms. Our analysis shows that between July and December 2017 Daesh used 145 platforms which were not used in the previous six months; and used approximately 400 unique platforms in 2017. Over 100 platforms have been used by Daesh so far in 2018 to disseminate and host propaganda online.

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?



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?



There is a small, manageable risk. However, automation technology can be trained to make a distinction between legal journalistic or counter-narrative content and terrorist propaganda. The Home Office developed technology with ASI Data Science that has been adversarially trained against educational and journalistic content to enable it to make this distinction. Tests have shown this new tool can automatically detect 94% of Daesh propaganda with 99.995% accuracy. This means an error rate of just 1 in 20,000.

Despite this, a process for redress is required to ensure that, if content is mistakenly identified as illegal content, it is not permanently removed from the platform.

II. 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?

It's a good start, but more must to be done to make the online space a hostile environment for terrorists to operate and to prevent the dissemination of terrorist content online. Engagement with and support for smaller companies is a critical priority.

In particular, we are seeing the threat moving to smaller platforms, and voluntary action has thus far not been able to stop it. UK analysis found that Daesh used 400 unique platforms over the course of 2017. 145 of those used in the second half of that year were platforms we'd not seen the group use before. This trend is continuing – over 100 platforms have been used by Daesh in 2018 to disseminate and host propaganda online.

The steps the EUIF is taking in terms of transparency reporting on online terrorist content are positive, however only 13 (out of 33 companies) presented data as part of the EUIF's latest transparency reporting.

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)?

Agree that EUIF's work should be further developed to make the online space a hostile environment for terrorists to operate and to prevent the dissemination of terrorist content online.

However, we must ensure that any action taken has a meaningful impact on the problem.

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)

X	More specific objectives for companies' actions (e.g. request a certain percentage of content taken down within a certain time limit)
X	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)
X	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 .
X	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)
X	More detailed requirements on transparency and reporting
X	More detailed requirements to companies on safeguards against over-removal
X	Establishment of an external audit/monitoring mechanism
X	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.
X	Additional support (e.g. by Europol) to referral capacities in Member States

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

Key measures set out above.

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

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 believe the most effective way is through industry-led engagement by larger CSPs. This is because they have the expertise to help, and also because small companies can be reluctant to engage with public authorities.

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:

⁴ See point 40 of the Recommendation.

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

III. Legislative options

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

The UK Government announced on 20 May that it will bring forward online safety legislation that would cover the full range of online harms, including online terrorist content.

Any action taken must:

- have a meaningful impact on the problem we are trying to solve, and must be more effective than the current voluntary approaches. We want companies to focus on:
 - transparency to ensure that effective measures are being taken by the companies to remove illegal content and to show compliance; and
 - speed of removals, as our research shows that approximately a third of all links to Daesh propaganda are disseminated within an hour of release;
- take into consideration smaller platforms which are increasingly being used to host and share online terrorist content as the larger companies have improved their response;
- be multi-jurisdictional; and
- be future proofed.

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 Directive⁵) is sufficient or should the dissemination of material pursuing other terrorist purposes be included as well?

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>

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
	Other, please elaborate:

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

Fully. In addition, the legislation should make provision to cover new and quickly evolving terrorist groups and their material. EU and UN lists are a valuable basis of reference, but we should be ready to react to material produced by new groups that are not yet officially prohibited. Consideration should also be given to groups proscribed in individual member states, such as National Action in the UK.

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)



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



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?

⁶ See point 41 of the Recommendation.

⁷ See points 16 and 17 of the Recommendation.

6. 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?

--

7. 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?

Article 6 of the Charter of Fundamental Rights of the European Union states that everyone has the right to liberty and security of person. Taking action against illegal content online aims to enhance security.

We are of the view that the impact on fundamental rights is negligible.