REPLY FROM SWEDEN 13 JUNE 2018

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 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	
Transparency rules	
Safeguards	

According to the Act on Responsibility of Electronic Bulletin Boards (1998:112), electronic bulletin boards (BBS) are defined as a service for mediation of electronic messages in the form of text, images, sound or other information. A supplier of a BBS is obliged to supervise the service to an extent that is reasonable considering the extent and objective of the service. The supplier is also obligated to remove a message, or in some other way make it inaccessible, if it is obvious that the content constitutes one of the following crimes: unlawful threat, unlawful violation of privacy, agitation against a national or ethnic group, inciting rebellion, unlawful depiction of violence, child pornography or intellectual property crime. A person who intentionally or by gross negligence, violates this obligation can be sentenced to a fine or to imprisonment for not more than six months, or, if the offence is grave, to imprisonment for not more than two years.

In Government Bill no. 2017/18:174, which has been submitted to the Parliament, but not yet voted on, the Government proposes the legislative measures deemed necessary to transpose the Directive 2017/514 on combating terrorism. As stated in the Bill, the Government considers that Swedish law is already in conformity with those provisions of Article 21 of the Directive that impose an obligation on the Member States. These provisions correspond to rules on seizure and confiscation that may be applied to e.g. servers, hard disks or domain names of websites containing content constituting a public provocation to commit a terrorist offence and, furthermore, to the Act on Responsibility for Electronic Bulletin Board However, for the purpose of clarification, the Government proposes to amend the Act on Responsibility for Electronic Bulletin Board by adding a reference to a more specific provision in the Act on Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serious Crime.

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)?

[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

No. However, the Secret Service are closely following the work of the Europol IRU. Indeed, it is among the responsibilities of a deployed liaison officer at Europol to maintain contact with the IRU in order to monitor developments and, where necessary and possible, cooperate.

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

For the time being, the opportunities offered by Swedish legislation within Swedish jurisdiction are considered sufficient together with the efforts made at EU-level to develop self-regulatory and voluntary measures. But, fighting and preventing illegal terrorism content online is obviously hampered by the truly border-less nature of the internet, i.e. the vast majority of such content accessed is connected with jurisdictions outside Sweden. Consequently, it is imperative that online platforms and hosting service providers that control the content take effective measures to counteract and remove illegal content on the basis of their respective community guidelines.

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?

Our general understanding from the very informative meetings and reports of the EUIF is that the presence of terrorism content is decreasing due to inter alia that Daesh is losing ground and that we now see clearer effects of the measures taken by the larger hosting service providers. However, we also understand that terrorism content is seeking new avenues and that smaller service providers are being abused.

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?

Yes, for instance intelligence gathering may be hampered the more content service providers are removing. But, on the other hand, it is precisely the objective of the EUIF that as much illegal terrorism content as possible is removed from the internet. Moreover, it seems to Sweden that this particular issue is quite horizontal and as such much concerned with improving the access to e-evidence and improving the cooperation between law enforcement and hosting service providers.

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?

Yes, hosting service providers may find themselves under pressure to remove content that may be legal according to EU-law or the law of a Member State, in particular if the content is referred from a law enforcement service of a Member State or from the Europol IRU. Hosting service providers may over-remove to "be on the safe side".

Furthermore, removal is at present ultimately based on community guidelines that might not always be in harmony with national or EU-law in defining what is illegal or not. This mismatch may lead to differences in the interpretation of what constitutes a breach of, on the one hand, the law of Member States and the EU, and, on the other hand, the respective community guidelines as laid down by each hosting service provider.

In our view, this risk is one of the major reasons why a clear distinction must be made between law enforcement services acting on the basis of law and hosting service providers acting on the basis of community guidelines. The relation between a law enforcement service and a service provider in the context of referral blurs this distinction, and risks undermining fundamental rights. States should not use informal means to circumvent the guarantees offered by formal legal proceedings.

There is also a need to further explore ways to ensure opportunities to challenge an alleged erroneous removal, for instance by means of a Code of Conduct on the part of service providers.

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?

The work of the EU Internet Forum has significantly contributed to a positive change in the level of commitment on the part of the hosting service providers as well as a readiness on the part of Member States, including Sweden, to seriously consider further action. The effects of the Recommendation are too early to assess, but the EUIF-report presented on 22 May indicates a very promising progress. It is an observable fact that the service providers have made real and substantial efforts and that clear improvements can be concluded.

We note that it has been a very rapid process from the Communication in September last year to a Recommendation on 1 March and now an impact assessment to establish if EU-legislation should be proposed or not. Our view is that the process too rapidly has reached the stage of an impact assessment. We believe that we should allow ourselves more time to assess and digest the progress made by hosting service providers as well as some important legal issues. Indeed, we think that we must also allow the hosting service providers more time to respond to our justifiable demands for action.

Furthermore, there are promising prospects for further progress on the horizon; Facebook and Youtube have for instance made commitments to reinforce their respective staff by 10.000 new employees dedicated to work against illegal content on

their platforms. Consequently, we are of the opinion that it cannot yet be concluded that it would be appropriate to seriously consider legislative action at EU-level, and, that therefore, the work under the EUIF as reinforced by the Recommendation is sufficient for the time being.

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)?

It seems to Sweden that an EU Code of Conduct with commitments on the part of the hosting service providers could be explored. Such a Code could strengthen the voluntary, self-regulatory measures significantly and address a number of specific concerns expressed in the EUIF as well as elements indicated in the boxes under III.3.

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)

4	More specific objectives for companies' actions (e.g. request a certain percentage of content taken down within a certain time limit).
5	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].
5	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)
5	More detailed requirements on transparency and reporting
5	More detailed requirements to companies on safeguards against over-removal
5	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.
4	Additional support (e.g. by Europol) to referral capacities in Member States. Comment: It could for instance be considered to organise expert meetings at Europol for coordination purposes and for the purpose to improve the overall understanding of the phenomenon among concerned EU law enforcement services.

[4] See point 40 of the Recommendation.

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

It seems to Sweden that all alternatives above under 3 include relevant elements for further discussion in a voluntary approach. However, and as noted elsewhere in this questionnaire, any measure, voluntary or legislative, must be assessed in view of its compatibility with fundamental rights and the rule of law.

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

Sweden agrees that this is a challenge, but note that progress is being made within the EUIF that also provides prospects for further improvements in this regard.

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?

Sweden agrees that this is a challenge, but note that progress is being made within the EUIF that also provides prospects for further improvements in this regard. Initiatives to support small companies as presented in the EUIF are important.

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. Comment: At least for the moment.
	No, it should be reinforced as presented above to obtain sufficient guarantees
	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?

There are according to Sweden some risks entailed by legislation at this time: 1. The process from a Communication via the Recommendation to legislation has been too fast. Can we, given the progress made, argue that we have pre-empted the voluntary approach? Can we conclude that we have given service providers enough time to respond to the calls of the EUIF, the Communication and the Recommendation? 2. There is a need to more carefully assess important elements of notice and action in relation to fundamental rights, for instance removal within one hour after referral from an authority that cannot establish in formal terms that the content is illegal or not seems to be one issue in need of further discussion. 3. A legislative proposal will jeopardise the momentum created by the EUIF.

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:

	Recruitment for terrorism
	Providing training for terrorism
	Terrorist financing
X	Other, please elaborate: The material scope of any EU-legislation must be based on definitions in national law or EU-law of what constitute terrorist content. Content that is not illegal is protected by fundamental rights.

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

It is irrelevant who is producing the material/content. The determining factor is whether the material/content is illegal or not.

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)

5	Definition of terrorist content (*see question above*)
5	Requirements regarding the companies' terms of service
5	General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)
x	Specific requirements in terms of action upon referral (including time limit of one hour)
x	More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)
x	Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms
x	Sanctions in case of non-compliance
x	Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material
5	Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)
x	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] 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

5	Nomination of point of contact within Companies
5	Reporting obligations for companies[6]
5	Transparency requirements for companies vis a vis their users[7]
x	Compulsory safeguards, such as the ones in the general chapter of the Recommendation
x	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?

As noted above, minimum, legal requirements risk disturbing the momentum established in the voluntary approach of the EUIF. If minimum, legal requirements are laid down, the incentive to take voluntary action may be lost.

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

Given the Swedish position, the boxes above under 3 are hypothetically ticked. The boxes ticked with x include issues that in our view requires further assessment and discussion. As pointed out elsewhere in this questionnaire, the relation between a law enforcement service and a hosting service provider offers particular challenges from the perspective of fundamental rights. We also hold this view when it comes to precisely which requirements to put on the hosting service providers and how far-reaching they could be, for instance forcing a co-operation between service providers, possibly sanctioned, appears to be a quite novel idea. Furthermore, it must be borne in mind that the issue concerning compulsory safeguards is not only a matter for the hosting service providers to provide, it may also involve considerations on the ways and means by which a complainant can seek legal redress against for instance a referral by a law enforcement service.

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?

It seems that one factor to consider here is what we know about how terrorism content is disseminated across the internet.

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?

Possibly yes, but this need further consideration, including on the basis of what we know about how terrorism content is spread across the internet and in which ways it reaches an audience.

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

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?

In particular the relation between a law enforcement service and a hosting service provider must be carefully assessed against the background of fundamental rights and the rule of law. A police or security service cannot, in a formal sense, establish that a particular content is illegal or not. Therefore, such a service can neither request or demand that a hosting service provider removes a certain piece of content in the context of a systematic work on notice and action without interfering with fundamental rights.

This is also the reason why Article 4.1(m) of the Europol Regulation underlines that the basis for removal must finally be the terms and conditions of the service provider: "support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions".

Furthermore, the mere threat of implications if a service provider is not removing content might hamper the market development and interfere with fundamental rights such as the freedom to conduct a business and freedom of expression and information. It is also important to consider that any content monitoring performed through automated means is unable to assess context properly. Inappropriately short timeframes for removal also risk working as an incentive for removal of legal content.

In summary, any regulatory approach must comply with the obligation to protect fundamental rights also online, including effective oversight mechanisms and appropriate legal redress opportunities.