EUROPEAN COMMISSION

Brussels, 12.9.2018
SEC(2018) 397 final

REGULATORY SCRUTINY BOARD OPINION

Proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online

{COM(2018) 640 final}
{SWD(2018) 408 final}
{SWD(2018) 409 final}

EUROPEAN COMMISSION
Regulatory Scrutiny Board

Brussels,
Ares(2018)

Opinion

Title: Impact Assessment / Illegal online content

(version of 06 July 2018)*

Overall opinion: POSITIVE WITH RESERVATIONS

(A) Context

There is a public interest in keeping illegal content off the internet. At the same time, freedom of expression is a fundamental right. Policymakers and courts have long balanced these interests.

Following recent terrorist attacks, many see a need for more immediate action. A few Member States are already responding. A set of EU regulatory and non-regulatory initiatives are putting in place solutions. The European Council and Parliament have called for industry and the Commission to ensure better detection and removal of content that incites terrorism. The same processes could also help to prevent other illegal content, e.g. hate speech, child sexual abuse material, piracy of intellectual property and selling illicit drugs. Better tech tools arguably make it possible to police content faster and more accurately.

This report examines ways to better detect and remove illegal content from the internet while respecting legitimate free speech and the common market.

(B) Main considerations

The Board notes services' commitments to redraft the report to reflect recent changes in this initiative's scope and context.

However, in its present form, the report contains significant shortcomings that need to be addressed. As a result, the Board expresses strong reservations and gives a positive opinion only on the understanding that the report shall be adjusted substantially in order to integrate the Board's recommendations on the following key aspects.

(1) The report does not adequately reflect that the initiative now focuses on illegal content linked to terrorism only. The report does not clearly establish an urgent need to act now at the EU level.

(2) The objectives do not reflect the balance between the development of the Digital Single Market, reducing terrorist content, and guaranteeing freedom of speech.

* Note that this opinion concerns a draft impact assessment report which may differ from the one adopted.

The report does not adequately explain how the legal basis for acting matches these objectives.

(3) The policy options do not reflect a more tightly scope linked to illegal terrorist content. They are not clear on which service providers they would cover and how they would include smaller platforms in a proportionate way. They do not adequately inform the policy choice.

(4) The report does not adequately establish that policy options are proportionate with regard to the fundamental right of freedom of expression and what safeguards are provided.

(C) Further considerations and adjustment requirements

(1) In line with the services' explanations to the RSB on recent changes in this initiative's scope and context, the report should **focus more narrowly on terrorist online content.** It should adjust the problem analysis, the policy objectives and the retained policy options accordingly. To justify the choice of scope, the report should explain why, despite numerous ongoing initiatives, there is a more urgent need to act now on terrorist content. It should report on the experience with measures already taken (voluntary) and on their limitations (e.g. limited participation of Internet platforms in voluntary programmes, hesitant cooperation of online platforms for combatting illegal content, difficult comparability of platforms' reporting). For a better understanding of the context, the report should also show how efforts to combat other illegal content are progressing, and why additional action is less urgent.

(2) The report should reshape the general and specific **objectives** to highlight the importance of the functioning of the Digital Single Market, the fight against terrorist online content, and the respect of freedom of speech. It should take into account the narrowing of the scope of the initiative from all illegal content to terrorist content

(3) On the basis of the redefined objectives, the report should provide a clearer justification for its **choice of the legal base**, i.e. Article 114 TFEU. The report should clearly demonstrate that the objectives can only be satisfactorily achieved under the selected legal base. It could better inform about consequences of selecting this legal base.

(4) In the light of the revised focus of the initiative on terrorist online content, the report should also revise the **baseline and the policy options**. The baseline should better project ongoing initiatives and possibly integrate elements now contained in the least ambitious option. The report should detail the policy options, indicating their component measures and highlighting how the options differ from each other. The report could define sub-options such that features of one policy option can also be useful in other policy options (e.g. designation of a competent authority). It should also indicate which type of Internet platforms are covered by each option, and to what extent specific provisions would apply to small service providers. Regarding the least ambitious option, several elements are arguably flanking measures that could be part of the revised options.

(5) The report should reinforce the assessment of the impact of the policy options on the development of the Digital Single Market and the fundamental right of **freedom of expression**. The initiative seeks to maintain a delicate balance between the freedom of expression, the respect of the eCommerce Directive and the combat against terrorism. Stakeholders have indicated that the fear of removal of legal content is a major concern to them. For each policy option, the impact analysis should clarify the safeguard measures that aim to ensure the freedom of expression. It particular, the report should be more

specific on the functioning and the precision of the automated content removal systems and the role of human intervention in these systems. The report should also endeavour to better inform the final policy choice by conducting a more rigorous comparison of the options.

(6) The report should better reflect the **views of stakeholders** with regard to the different problems and policy options. It should be transparent about which parts of the consultation are relevant for the narrower focus on terrorist online content.

(7) The attached quantification tables of the various costs and benefits associated to the options of this initiative need to be adjusted to reflect the changes recommended above.

Some more technical comments have been transmitted directly to the author DG.

(D) RSB scrutiny process

The lead DG shall ensure that the report is adjusted in accordance with the recommendations of the Board prior to launching the interservice consultation.

The attached quantification tables may need to be further adjusted to reflect changes in the choice or the design of the preferred option(s) in the final version of the report.

Full title	Impact assessment accompanying the document: measures to improve the effectiveness of the fight against illegal (terrorist) content in the Digital Single Market
Reference number	PLAN/2017/1766
Date of RSB meeting	24/07/2018

ANNEX: Quantification tables extracted from the draft impact assessment report submitted to the Board on 06/07/2018

(N.B. The following tables present information on the costs and benefits of the initiative in question. These tables have been extracted from the draft impact assessment report submitted to the Regulatory Scrutiny Board on which the Board has given the opinion presented above. It is possible, therefore, that the content of the tables presented below are different from those in the final version of the impact assessment report published by the Commission as the draft report may have been revised in line with the Board's recommendations.)

Option 1

Overview of Benefits Option 1	
Description	***Benefits***
Direct benefits	
For hosting services	Additional technological tools, know-how and best-practices available at low cost. Flexibility of the voluntary system to adapt best practices to the specific business models.
For **public authorities**	Flexible voluntary dialogues allow addressing the different problems with the varied types of illegal content as they evolve.
For **trusted flagger entities**	Investment in training and capacity building will lead to enhanced capacities of trusted flaggers.
Indirect benefits	
For **civil society**	Increased participation and accountability in the design of new approaches to fighting illegal content
For **3rd party technology providers**	Possible creation of an incentive for a market for technology solutions for content moderation at scale

Overview of costs – Option 1							
		Citizens/Consumers		Businesses		Public administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Technology Development	Direct costs	none	none	none	none	~ 15 FTE for setting up and maintaining a shared database and cooperation tools (over 2 years), for Europol	~ 5FTE for running the system
	Indirect costs	none	None			none	none
Public R&D on spread of illegal content	Direct costs	none	None	none	None	From baseline EU funding	From baseline EU funding
	Indirect costs	none	none	none	none	From baseline EU funding	From baseline EU funding
Trusted Flagger System	Direct costs	None	None	None	None	From baseline EU funding	100kEUR for 2 annual meetings + 100kEUR for

							training and capacity building
	Indirect costs	None	None	None	None	None	None
Reinforcement of dialogues	Direct costs	None	None	None	None	None	None
	Indirect costs	None	None	None	None	None	None

Option 2 & sub-options

Overview of Benefits Option 2	
Description	***Benefits***
Direct benefits	
For **hosting services**	Under all sub-options, harmonised rules should counter fragmentation of the Internal Market and increase legal certainty and trust. Service providers protected against being misused for terrorist purposes.
For **public authorities**	Reinforced ability of competent authorities and Europol to monitor effectiveness of action taken against terrorist content online and to take appropriate measures against the dissemination of terrorist content and terrorist activity in general (notably in options 2B and 2C)
For **internet users**	Safety of users will be improved, reducing the risk of being exposed to terrorist material and reducing the risks for individuals who may be vulnerable to recruitment to terrorism (notably in options 2B and 2C)

Indirect benefits	
For **citizens and society at large**	Increased security of EU citizens and the society at large.
For civil society	Further clarity as to the role and actions taken by competent authorities and service providers.
For **3rd party technology providers**	Creation of a market for the development of automatic content detection, filtering and moderation technologies.

Overview of costs – Option 2

With regards to the costs, some of the measures have been adjusted to take into account, where appropriate, the size of the company, the possible exposure to risk (likely to be determined based on the number of removal orders) An approximate cost on both hosting service providers and public administration is presented below taking into account the differences between the various sub-options.

Measures		Sub-option A		Sub-option B		Sub-option C	
		Hosting service providers	Public administrations	Hosting service providers	Public administrations	Hosting service providers	Public administrations
Action upon	Measures for 1h removal for HSPs (range based on	0.5 – 4 FTEs for companies depending on degree of	Small one off costs for adapting to new	0.5 – 4 FTEs for companies depending	Small one off costs for adapting to new	0.5 – 4 FTEs for companies	Small one off costs for adapting to new

Measures		Sub-option A		Sub-option B		Sub-option C	
		Hosting service providers	Public administrations	Hosting service providers	Public administrations	Hosting service providers	Public administrations
removal order	micro, small companies having a 24 h deadline)	assessment needed, and whether mere technical interventions as part of normal continuity procedures can accommodate the order + small one-off costs to establish procedure	procedures	on degree of assessment needed, and whether mere technical interventions as part of normal continuity procedures can accommodate the order + small one-off costs to establish procedure	procedures	depending on degree of assessment needed, and whether mere technical interventions as part of normal continuity procedures can accommodate the order + small one-off costs to establish procedure	procedures
	Designation of competent authorities and assessing feedback from companies		Absorbed in the baseline as there is no obligation to establish an IRU		Absorbed in the baseline as there is no obligation to establish an IRU		Obligation to establish will lead to a cost of 1 "IRU" per 23 Member State estimated at average ~3FTEs + 20 000 running costs
Action upon Europol referrals	Measures for 12 h removal for HSPs(range based on micro, small companies having a 24 h deadline)	None	None	absorbed in removal order costs to – 2.5 FTEs on top of existing moderation system to guarantee 12 hours (depending on volume	None	Same as option A	None

Measures		Sub-option A		Sub-option B		Sub-option C	
		Hosting service providers	Public administrations	Hosting service providers	Public administrations	Hosting service providers	Public administrations
				of referrals) + one-off training (4 days) on Europol referrals			
	Measures for 6 h removal for HSPs (range based on micro, small companies having a 24 h deadline)	None	None	None	None	absorbed in removal order costs to – 5.5 FTEs on top of in existing moderation system to guarantee 6 hours (depending on volume of referrals) + one-off training (4 days) on Europol referrals	None
Proactive measures							
	Risk assessment	= 3 days / year training with EUROPOL incl. risk assessment for 3 staff (technical, moderation, legal)	1 Europol/0,5 x 5 National authority experts for assistance to companies for risk assessment	= 3 days to carry out incl. risk assessment with 3 staff (technical, moderation, legal)	0.5 Europol/National authority experts for assistance to companies, if need be, for risk assessment	None	None

Measures		Sub-option A		Sub-option B		Sub-option C	
		Hosting service providers	Public administrations	Hosting service providers	Public administrations	Hosting service providers	Public administrations
	Cooperate with Europol and Member States to reinforce effectiveness of mitigating measures	None	None	Absorbed by other costs	0,5 FTE x 5 national authorities 1 FTE in Europol	None	None
	Prevent re-upload of already removed terrorist content	None	None	Cost of in-house manual, semi-automatic, or automatic filtering systems to prevent re-upload + cost maintenance (for companies at high risk and according to their size)	None	cost of in-house manual, semi-automatic, or automatic filtering systems to prevent re-upload + cost maintenance	0,5 FTE in Europol for monitoring
	Use of technical tools to detect and prevent accessibility of new terrorist content	None	None	OR cost of access to a shared database of hashes + contribution to maintenance	None		0,5 FTE in Europol for monitoring
	Indirect costs	None	None	None	None	None	None
Cooperation	Points of contact for	= baseline legal staff for	None	= baseline legal staff for	None	= baseline legal staff	None

Measures		Sub-option A		Sub-option B		Sub-option C	
		Hosting service providers	Public administrations	Hosting service providers	Public administrations	Hosting service providers	Public administrations
between national authorities (and HSPs) and Europol	HSPs	HSP		HSP		for HSP	
	Informing Europol of actions taken	None	= baseline + marginal additional cost for electronic information	None	= baseline + marginal additional cost for electronic information	None	= baseline + marginal additional cost for electronic information
Requirement to maintain accessibility of terrorist content for law enforcement purposes	Reporting obligation	= 0.25 FTE to 1 FTE for assessment of content to report + marginal additional cost for electronic information	Significant cost depending on volumes reported and authorities' policies	None	None	None	None
	Retention obligation	None	None	~ baseline + 0.25 FTE technical staff and storage costs; GDPR compliance costs assumed to be baseline costs; costs can be higher for some specialised HSP depending on their business model	None	~ baseline + 0.25 FTE technical staff and storage costs; GDPR compliance costs assumed to be baseline costs; costs can be higher for some specialised HSP depending on their business model	None

Measures		Sub-option A		Sub-option B		Sub-option C	
		Hosting service providers	Public administrations	Hosting service providers	Public administrations	Hosting service providers	Public administrations
Safeguards	Complaint procedures and judicial redress	~ baseline + 0,25-1 FTE for complaint handling	None	~ baseline + 0,25-1 FTE for complaint handling	None	~ baseline + 0,25-1 FTE for complaint handling	None
	Transparency		None	absorbed in overall system	None	absorbed in overall system	None
	Reporting to the Commission	~ contained in the system costs	0,25FTE for reporting	~ contained in the system costs	0,25FTE for reporting	~ contained in the system costs	Absorbed in the IRU costs
Enforcement	Requirement to establish a legal representative (for companies established outside the EU)	~ baseline (included e-evidence Legal Rep) + 50kEUR running costs	None	~ baseline (included e-evidence Legal Rep) + 50kEUR running costs	None	~ baseline (included e-evidence Legal Rep) + 50kEUR running costs	None
	Monitoring and sanctions		0,25 FTE per MS		0,25 FTE per MS		Absorbed in the IRU costs
Establishment of EUIF as permanent consultative forum		None	From baseline + EU funding	None	From baseline + EU funding	None	From baseline + EU funding

Option 3

Overview of Benefits Option 3	
Description	***Amount***
Direct benefits	
For **hosting services**	Legal certainty and harmonised requirements across 28 jurisdictions would make it easier for offering services across the Single Market to comply.
For **public authorities**	Enforced monitoring capacity and overview on the volumes of illegal content and effectiveness of takedown
Indirect benefits	
For **consumers and users of hosting services**	Better protection against all types of illegal content Transparency and increased predictability when their content is erroneously taken down
For **third-party content moderation services**	Legal requirements for notice & action systems can lead to a higher demand on the market for such services Current offers range from base price of 4000 EUR per annum to 50 000EUR and much higher, depending on volumes of content analysed

Overview of costs – Option 3							
		Citizens/Consumers		Hosting service providers		Administrations and third parties sending notices (e.g. trusted flaggers)	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Harmonized Notice and Action (N&A) and counter-notice systems	Direct costs	none	none	from 15 000 EUR per year (for provision and maintenance of a simple web form), to 500 000EUR per year (for differentiated access for trusted flaggers on e-commerce platforms)[1]	Skilled personnel to treat notices, ranging from minimum 0.4 FTE to assess and expedite notices, to 1600 FTEs[2], depending on the size of the company, volumes of content, as well as fluctuations in illegal activity.	For entities issuing notices: Minor costs to adapt to standardised notice forms.	none
	Indirect costs	none	Minor risk of limited cost transfer on particular cases	none	none	none	none

[1] Cf. ICF study reported data from interviews with hosting services

[2] Estimates based on lowest and highest volumes of notices reported by companies publishing a transparency report in 2017. One FTE estimated to process up to 20.000 notices a year. Companies have reported, however, up to 10. 000 FTEs for content moderation, all functions included

Information to content providers (under certain conditions)	Direct costs	none	none	Absorbed in the N&A costs	Absorbed in the N&A costs	none	none
	Indirect costs	none	none	none	none	none	none
Point of contact within the EU	Direct costs	none	none	Unlikely limited costs for setting up the point of contact	Maximum 30 working days for the legal representative designated or contracted.[3]	none	none
	Indirect costs	none	none	none	none	none	none
Annual transparency reports and ad-hoc	Direct costs	none	none	Expected to be absorbed in the N&A set-up system	0.1 FTE for reporting	none	none

[3] It is expected that most of these companies would have already established a point of contact following provisions of legal instruments such as the General Data Protection Regulation or the proposal on the production and preservation of orders for electronic evidence in criminal matters, and some cost savings could result from the accumulation of functions.

reporting to national authorities	Indirect costs	none	none	none	none	none	none
MS reporting to the Commission	Direct costs	none	none	none	none	none	MS: Not more than 0.2 FTEs for reporting
	Indirect costs	none	none	none	none	none	none
Public monitoring and enforcement	Direct costs	none	none	none	none	none	1 FTE
	Indirect costs	none	none	none	none	none	none
Total::	For hosting services - scenarios: ~baseline + 0.5 FTEs (expected for small companies, not specifically targeted by any kind of illegal activity) + potentially, min. 15000EUR to set-up a notice & action system ~baseline, including increase of FTEs up to 1600 For Member States and National authorities: limited costs for enforcement, monitoring and reporting, ~1.2 FTEs						