

A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries

Questions marked with an asterisk * require an answer to be given.

Introduction

The **E-commerce Directive** provides a framework for the cross-border provision of online services in Europe. It includes so-called exemptions from liability for online "intermediary service providers". In particular, it provides that online service providers may not be held liable for illegal content that they "host" on condition that:

- the provider does not have 'actual knowledge' of illegal content and is not 'aware' of facts or circumstances from which the illegal content is apparent; or
- the provider, upon obtaining such knowledge or awareness acts 'expeditiously' to remove or disable access to the content (Article 14 E-commerce Directive).

This rule forms the basis for so-called "notice-and-action" (N&A) procedures. These procedures start whenever someone "*notifies*" a hosting service provider about illegal content on the internet. The procedures are concluded when an online intermediary *acts* against the alleged illegal content. Acting may take the form of removing or disabling access to the illegal content.

In 2010 the Commission held a public consultation on the future of e-commerce and the implementation of the E-commerce Directive. The vast majority of the 420 respondents considered that the principles contained in the E-commerce Directive are still valid and asked the Commission not to propose a revision of the Directive. However, many respondents asked for clarifications of certain articles in the Directive, notably Article 14 and the functioning of N&A procedures. The consultation made clear that respondents consider that there are three main problems with the functioning of N&A procedures:

- online intermediaries face high compliance costs and legal uncertainty because they typically have operations across Europe, but the basic rules of Article 14 are interpreted in different ways by different national courts (sometimes even within the same Member State). In particular the terms "actual knowledge", "awareness" and "expeditiously" have led to diverging national case-law. Notice providers and hosting providers have to adapt their practices in accordance with these interpretations.
- illegal content stays online too long. This is partly due to what is perceived as a lack of sufficiently clear rules and easily identifiable procedures.
- fundamental rights are not always respected. In particular, there are instances where legal content is taken down, which can amount to a restriction of the right to freedom of expression and information. This arises partly as a result of liability fears on the part of hosting providers and the fact that the providers of alleged illegal content are in general not consulted before a hosting service provider takes action.

In order to address these challenges, the Commission announced an initiative on N&A procedures in the **Communication** on e-commerce and other online services. The **Staff Working Paper** accompanying the Communication presents an overview of the implementation of Article 14 and the functioning of N&A procedures in the EU. Subsequently, the Commission engaged in a fact-finding exercise on notice-and-action procedures which included targeted stakeholder consultations. The

Commission now wishes to obtain the view of all stakeholders on specific issues related to the functioning of N&A procedures in Europe in the context of Article 14 of the E-commerce Directive. The responses will assist the Commission in shaping the N&A initiative.

The public consultation is available in English, French and German. Responses can be in any of the 23 official languages of the EU, but replying in English, French or German would enable Commission services to process them more quickly. Answers to the questions must be sent by using the electronic application 'IPM' (Interactive Policy Making). The electronic version of the public consultation is available **here**. The views expressed in this public consultation may not be interpreted as stating an official position of the European Commission.

Glossary

- **"(Online) intermediary service providers"** provide online service¹ that consist of transmitting or storing content that has been provided by a third country, the E-commerce Directive distinguishes three types of intermediary services: mere conduit (transmitting of data by an internet access provider), caching (i.e. automatically making temporary copies of web data to speed up technical processes) and hosting (see below).
- **"Illegal content"** corresponds to the term "illegal activity or information" used in Article 14 of the E-commerce Directive. This directive does not further specify this term. It may be understood in a wide sense so as to include any infringement of applicable EU or national laws and regulations. This could for instance include defamation terrorism related content, IPR infringements, illegal online gambling, child abuse content, misleading advertisements or incitement to hatred or violence on the basis of race, origin, religion, gender, sexual orientation etc.
- **"Hosting"**, according to Article 14 of the E-commerce Directive, is the "storage of (content) that has been provided by the user of an online service". It may for instance be storage of websites on servers. It may also include the services offered by online market places, referencing services and social networks.
- A **"notice provider"** is anyone (a natural or legal person) that informs a hosting service provider about illegal content on the internet. It may for instance be an individual citizen, a hotline or a holder of intellectual property rights. In certain cases it may also include public authorities.
- A **"notice"** is any communication to a hosting service provider that could give the latter knowledge of a particular item of illegal content that it hosts. It could therefore create an obligation for it to act expeditiously by removing the illegal content or disabling/blocking access to it if the provider wishes to be exempted from liability under Article 14 of the E-commerce Directive. Such an obligation only arises if the notice provides the hosting service provider with actual knowledge of illegal content.
- A **"provider of content"** in the context of a hosting service is the user of that service. A provider of content is for instance someone who posts a comment on a social network site or uploads a video on a video sharing site.

¹ The E-commerce Directive uses the term "information society service".

- **"Action"**, for the purpose of this consultation, means removing (taking down) or disabling access to illegal content. According to Article 14 of the E-commerce Directive, if the provider wishes to be exempted from liability, a hosting service provider should act "to remove or disable access" to illegal content once the provider becomes aware of it.

I. Background information

This consultation is addressed to the public in general/broadest public possible, as it is important to get the views and input from all the interested parties and stakeholders. In order to best analyse the responses received after the consultation, and to maximize their usefulness, we need to have a limited amount of background about you as a respondent.

1. Please indicate your role for the purpose of this consultation: *	
Individual	Public authority / law enforcement
Civil society association	Intellectual property rights
Hosting service provider	<input checked="" type="checkbox"/> Business federation
Internet access provider	Research institution / Think tank
Private company (not hosting service provider of internet access provider)	Other
Hotline	

Please specify:

ETNO has 40 member companies from 35 European countries, representing a significant proportion of aggregate information and communication technology (ICT) activity in Europe. The members account for a combined annual turnover of more than €250 billion and employ over one million people across Europe. ETNO companies are the main drivers of broadband growth, having accounted for two thirds of total high-speed broadband deployment to date. Besides their specific role as network and Internet access providers, ETNO members also offer hosting services. In addition to this, many of them are also content providers. As such, they are active in the promotion and provision of legal content services over their networks. Within this framework, they already provide efficient Notice and Action (N&A) mechanisms, according to national legislation in place.

ETNO has been actively contributing to the debate on illegal activities and illegal content hosted online and, in particular, on how to improve, in a proportionate and appropriate way, mechanisms designed to address this issue. ETNO, as well as some of its members in their individual capacity, has provided the Commission with more specific information on this issue prior to the current consultation. Nonetheless, ETNO welcomes the current consultation as a means of reiterating its position and pointing out some additional considerations.

In particular, we reiterate that:

- ETNO members are particularly active in promoting a fair and safe Internet environment in all relevant fields and in particular as regards the protection of children and minors. Many of ETNO's members are part of ongoing EU initiatives such as the Safer Internet, the Mobile Alliance, the ICT Child Safety Principles and the recently established CEO coalition to make Internet a better place for children. They are also part of initiatives at national level.
- There are huge differences between various unlawful activities/content that can be found online, and the related social value and economic impact. There cannot be a 'one size fits all' solution.

- In order to guarantee a safe and sound Internet environment, it is of utmost importance that efficient procedures for N&A are implemented by hosting service providers (“HSP”). Examples of such mechanisms which have already been efficiently developed and implemented, mainly voluntarily, by European HSPs do exist.
- Concerning Intellectual Property Rights (IPR) protection, ETNO members, while fully recognizing the need for rights-holders to receive fair remuneration, believe that attractive legal offers and innovative business ideas would increase revenues for rights-holders while help address the issue of digital infringement of copyright.
- ETNO members are also fully committed to guaranteeing secure communications networks and services and are closely following the discussions and initiatives that are ongoing at EU and national level.
- Intermediaries and HSPs in particular cannot reasonably replace legal authorities in assessing the legality/illegality of conduct or content that has been notified as being allegedly illegal. This would imply taking up a role and responsibilities that hosting providers cannot assume.

Against this background:

- We believe that any intention to adopt a horizontal approach when proposing a measure on N&A raises serious concerns as one has to consider the differences that exist between various illegal activities and behaviour types online. The Commission should focus its efforts on fostering the voluntary adoption and improvement of N&A mechanisms already implemented by EU intermediaries and, if necessary, guidelines may be issued aimed at interpreting those provisions which still raise uncertainties and result in substantially fragmented approaches.
- In line with the conclusions reached by the Commission on a number of occasions, ETNO strongly believes that the e-Commerce Directive already contains sufficiently specific and clear provisions on intermediary liability and therefore a legislative revision would not be justified. Final guidelines on N&A should comply with the spirit of the e-Commerce Directive spirit and any new measure – also of a soft law nature - should be proportionate, taking into account the interests of the different stakeholders and the objective, which may vary depending upon the illegal activity at stake.
- If any new mechanisms are to be introduced, their effectiveness should be ensured. In this respect, any N&A mechanism should cover those content/behaviours which are clearly found to be unlawful and should not be extended to “inappropriate” content or behaviors. In addition, it is important to note that at European and national levels, there are different legal frameworks already applicable to specific illegal activities, such as in the field of child protection (ex. the recent European Directive) and illegal online gambling. Thus, substantial efforts from the European institutions are needed in terms of coordination.
- Any N&A procedure should be limited to hosting and should provide different safeguards for different types of content. We do not support N&A aimed at imposing generalized mandatory web blocking and network filtering, which we strongly oppose.
- While Child Abuse Material may deserve specific and rapid action, including a discussion on its specific challenges and discussions for improvement, any other notification should be validated by a third party (e.g. a court, Government-appointed officials or other independent third party) *before* a HSP can be required to act on it. This is so as to remove the HSP from having to evaluate the validity of the notification, which would have heavy consequences in the case of (inadvertent) removal of legal content, not only in terms of HSP liability vis-à-vis customers, but also in terms of a violation of fundamental rights, such as the freedom of speech.
- We do not support mandatory “notice-and-stay-down” procedures for hosting in particular, as this implies a general monitoring obligation which also, aside from being in violation of the applicable rules, would be costly, difficult to implement and technically not fully reliable.
- We do not believe that blocking should be the preferred solution to eradicate illegal content. Blocking requires significant resources and its effectiveness is questionable as it can be easily circumvented. In addition, if blocking is not exercised properly it can harm human rights. Blocking

orders may lead to the blocking of legal content that is not intended to be blocked and should be therefore restricted to exceptional and circumstantiated cases. Indeed it carries the added risk of over-blocking both from a domain name perspective (blocking sub-domains legal sites) and a geographic perspective due to the configuration of some networks – particularly pan-European (i.e. depending on the location of servers an ISP may end up over-blocking sites in another jurisdiction). This “over-blocking” problem risks the denial of rights to innocent websites unrelated to the unlawful content that is the target of the notification and raises concerns as to the proportionality of the measure compared to less restrictive alternatives. Therefore, blocking must be used with extreme caution, when other solutions have been exhausted and have failed and only after a fully justified and well defined order.

- There should be clear legal framework governing the exercise of powers to suspend services, with adequate safeguards both for HSP and for the citizens of the country in question. In any case, the conditions under which the blocking activity could occur must be carefully considered and clearly specified, in order not to be contrary to fundamental rights such as the freedom of speech, or to go against fundamental services such as the emergency services.

In conclusion, a viable solution may be a “notice-and-notice” mechanism, provided that, having received the notification, the hosting provider, without undue delay, should notify it to the competent public authority in charge of assessing the illegality of the alleged conduct/content and being competent to address the subsequent decision to the hosting provider. This would also allow the competent authority to contact the alleged infringer for clarifications before reaching a decision, giving the alleged infringer an opportunity to object to the eventual takedown demands (“counter-notice”). The hosting provider, upon receipt of the notification of illegal content validated by the competent public authority, should start the removal process expeditiously.

A N&N approach can be managed with a reasonable degree of technical difficulty and it would have the substantial benefit of implying a very reduced cost for the entity hosting the content and for the industry as a whole compared to other options such as ISP blocking, while being efficient in terms of fighting against illegal content/activities over the Internet. A N&N solution does not require a broad court order issued to all ISPs in the country, rather the order can be directed to the entity that actually hosts the content.

2. Please indicate your place of residence or establishment: *		
Austria	Finland	Poland
<input checked="" type="checkbox"/> Belgium	France	Portugal
Bulgaria	Hungary	Romania
Czech Republic	Ireland	Slovakia
Cyprus	Italy	Slovenia
Germany	Lithuania	Sweden
Denmark	Luxembourg	United-Kingdom
Estonia	Latvia	EU association
Greece	Malta	Non-EU country
Spain	The Netherlands	Other

Please specify:

ETNO’s field of activity is particularly focused on European policy issues. Therefore, it has its legal base in Brussels, Belgium.

--

Please specify:

3. Please provide your contact information (name, address and e-mail address): *
Caterina Bortolini Corso d'Italia 41, 00198 Rome, Italy caterina.bortolini@telecomitalia.it
Caroline Greer Avenue Louise 54, Brussels 1050, Belgium greer@etno.be

4. Is your organization registered in the Interest representative Register? *
<input checked="" type="checkbox"/> Yes
<input type="checkbox"/> No
<input type="checkbox"/> Not relevant

5. What is/are the category/ies if illegal content of greatest relevance to you in the context of N&A procedures? *
<input type="checkbox"/> Illegal offer of goods and services (e.g. illegal arms, fake medicines, unauthorized gambling services etc.)
<input type="checkbox"/> Illegal promotion of goods and services
<input type="checkbox"/> Content facilitating phishing, pharming or hacking
<input checked="" type="checkbox"/> Infringements of copyright and related rights
<input type="checkbox"/> Infringements of trademarks
<input type="checkbox"/> Infringements of consumer protection rules
<input type="checkbox"/> Incitement to hatred or violence (on the basis of race , religion, gender, sexual orientation etc.)
<input checked="" type="checkbox"/> Child abuse content
<input checked="" type="checkbox"/> Terrorism related content (e.g. content inciting the commitment of terrorist offences and training material)
<input checked="" type="checkbox"/> Defamation
<input checked="" type="checkbox"/> Privacy infringements
<input checked="" type="checkbox"/> Other: cybercrimes, illegal online gambling
<input type="checkbox"/> Not applicable

Please specify:
The Commission's intention to adopt a horizontal approach when proposing a measure on N&A raises serious concerns if one considers the huge differences that exist between various types of

illegal activities/content that can be carried out online, and so there is a resultant difference in the related social value and economic impact. There cannot be a one size fits all solution. This is mirrored at European and national level, where there are different legal frameworks already applicable to specific illegal activities, such as in the field of child protection (eg. the recent European Directive and the ongoing CEO Coalition initiative to make the Internet a better place for children) and illegal online gambling. Measures that can be proportionate when implemented with the aim of protecting children or fighting terrorism, cannot be justified under the proportionality test if applied to other online illegal activities/content.

With particular reference to privacy infringements, we note that social networks or video platforms can also be a means for third party privacy infringements. Due to the growing success of these services, the risks of being liable are a reality and can undermine innovative services. Hosting service providers should be liable for privacy infringements committed by third parties on their platforms under art 14 of the e-Commerce Directive.

II. Notice and Action procedures in Europe

In 2010 the Commission consulted the public on the future of e-commerce and the implementation of the E-commerce Directive. The public consultation included questions on the liability exemptions for online intermediaries, the interpretation of Article 14 of the E-commerce Directive and notice-and-action procedures. These responses have been reflected in a **Staff Working Paper** accompanying the E-commerce Communication.

Many of these responses indicated that there are difficulties with the interpretation of Article 14 of the E-commerce Directive. Article 14 defines hosting as *"an information society service (..) that consists of the storage of information provided by a recipient of the service"*. It provides that a provider shall not be liable for hosted illegal content on condition that:

"a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information" The Commission would now like to have an updated vision of stakeholders regarding notice-and-action procedures".

The Commission now would like to obtain an updated vision of stakeholders regarding notice-and-action procedures in the context of Article 14 of the E-commerce Directive.

6. To what extent do you agree with the following statements on notice-and-action procedures?					
	a	b	c	d	e
a. I completely agree					
b. I agree					
c. I disagree					
d. I completely disagree					
e. No option					
Action against illegal content is often ineffective			X		

Action against illegal content is often too slow			X		
Hosting service providers often take action against legal content			X		
There is too much legal fragmentation and uncertainty for hosting service providers and notice providers			X		

7. To what extent do you agree with the following statements on Article 14 of the E-commerce Directive?					
a. I completely agree					
b. I agree					
c. I disagree					
d. I completely disagree					
e. No opinion					
	a	b	c	d	e
The exact scope of "hosting" is sufficiently clear		X			
The terms "actual knowledge" and "awareness" are sufficiently clear		X			
The term "expeditiously" is sufficiently clear		X			

The public consultation on e-commerce of 2010 has demonstrated that most stakeholders consider hosting of <i>websites</i> to be hosting, but that there is less unanimity on other services that could be hosting. The CJEU has stated that hosting may in principle be the services of online market places, referencing services and social networks.	
8. In your opinion, what activities should be considered as "hosting"?*	
X Social networks	X Blogs and interactive dictionaries
X Video-sharing sites	X Cloud based services
X E-commerce platforms	Other
X Search engines	None of the above
X Cyberlockers	No opinion

Please specify:

A hosting service – and a HSP - is well defined in Art.14 of the e-Commerce directive (i.e “the storage of information provided by a recipient”). A number of decisions have subsequently been taken by several national bodies and also by the European Court to specify the definition. In particular, the CJEU has established a broad interpretation of the hosting definition including social networks, online market places and referencing services. The natural extension of such a definition should include video-sharing sites, search engines, blogs and interactive dictionaries.

In some countries, national courts have highlighted the difference between a passive hosting service provider, which falls within the liability exemption provided for by Art. 14 of the Directive, and an active hosting provider that does not fall within the exemption.

In particular, new emerging cloud-based services which consist mainly of the storage of information

provided by a third party, with no control or management activity of the said information by the provider, subsequently qualify as a hosting service and the exemption liability regime for the provider applies.

III. Notifying illegal content to hosting service providers

The E-commerce Directive does not use the terms "notifying" or "notice". The CJEU has clarified that one possible way to become aware of illegal content is that a hosting service provider is "notified" of such content. However, the CJEU has held that a notice cannot automatically lead to awareness of illegal content. If the notice is "insufficiently precise or inadequately substantiated" the notice does not make the hosting service provider aware of illegal content².

EU law does not contain rules on the availability and accessibility of means to notify as referred to above. Some notice providers, however, have complained that mechanisms for notifying illegal content are not always in place or not always easy to use or to find.

9. To what extent do you agree with the following statements?					
a. I completely					
b. I agree					
c. I disagree					
d. I completely disagree					
e. No opinion					
	a	b	c	d	e
It is easy to find pages or tools to notify illegal content?		X			
It is easy to use pages or tools to notify illegal content?		X			

10. Should all hosting service providers have a procedure in place which allows them to be easily notified of illegal content that they may be hosting? *	
<input checked="" type="checkbox"/> Yes	
<input type="checkbox"/> No	
<input type="checkbox"/> No opinion	

Please specify:

Many European content platforms and other HSPs, including ETNO members, have already developed their own efficient notice practices based on experiences specific to their diversified businesses. In the future, such tools will be even further adopted in a voluntary way, also as part of a business strategy aimed at providing services of increased quality and with a rights protection viewpoint.

Others work within a system where public authorities work closely with HSPs to ensure an efficient and smooth process.

² Judgment of the Court of Justice of the European Union of 12 July 2011 in case C-324/09 (L'Oréal – eBay), points 121-122

Some hosting service providers have voluntarily put in place mechanisms to receive notifications of illegal content.

Some of these providers have complained that their mechanisms are not always used and that concerns about content are not notified in a manner that would be easy to process (e.g. by fax, without sufficient information to assess the alleged illegal character of content etc.). Providers also claim that this creates delays in taking action against illegal content, because the hosting service provider would for instance have to contact the notice provider to ask for additional information.

11. If a hosting service provider has a procedure for notifying illegal content (such as a web form designed for that purpose) that is easy to find and easy to use, should illegal content exclusively be notified by means of that procedure? *

Yes

No

No opinion

Please explain:

Usually, the notification tools developed by ETNO members are accessible via their portal or a forum web page. This may also include notification links that transfer directly to an appropriate body depending on the category of illegal content (e.g. an NGO taking care of reports on child abuse material). The use of these existing tools makes procedures easier to follow and quicker to apply. Internet users are therefore able to notify illicit content such as child abuse material in the most user-friendly and speedy way. In some Member States, these notification processes are optimized for the specific intermediary platform and tailored to the categories of content to be notified. The objective is to gather relevant data to act efficiently against the illegal content addressed (contact of the notice provider, time and date of alleged infringement, URL, description of the infringement,...). Having a minimum set of information to be supplied to the hosting provider will help the process.

We believe that using intermediary notification systems is the easiest way for the notice provider to inform the hosting service provider and/or relevant authorities about the alleged existence of illegal content or behavior online.

In addition, we note that when violations of IPRs are at stake, rights-owners tend to prefer to use – with no particular apparent reason - other forms of notification, often not using electronic means but delaying the efficient online treatment of the notice and thus jeopardizing the entire system. However, we strongly believe that EU policy-makers should support, encourage and, where appropriate, facilitate the widespread use and adoption of N&A as already developed and implemented by hosting providers as the most effective and proportionate means of tackling alleged illegal content.

Certainly, a degree of flexibility should be allowed, to enable hosting service providers to determine their own appropriate standards of notification. In cases where the notice provider informs the hosting service provider by other means than those proposed, it will not be ignored but may cause unnecessary delays.

Although the CJEU indicated that a notice should be sufficiently precise and adequately substantiated to have effect, it has not indicated how these requirements should be met for this

purpose. Nor has this been specified in the E-commerce Directive.

12. Do you agree with the following statements?

	Yes	No	No opinion
A notice should be submitted by electronic means	X		
A notice should contain contact details of the sender	X		
A notice should make it easy to identify the alleged illegal content (for instance by providing a URL)	X		
A notice should contain a detailed description of the alleged illegal nature of the content	X		
A notice should contain evidence that the content provider could not be contacted before contacting the hosting service provider or that the content provider was contacted first but did not act.	X		

Can you please specify why you do not agree with the statement: "A notice should be submitted by electronic means"

N/a

Can you please specify why you do **not** agree with the statement: "A notice should contain contact details of the sender"

Although we have agreed with this statement, we would like to note that in some Member States, specifically in cases of child-pornography related crimes, national legislation allows the sender to remain anonymous. This allows for the protection of those users that come across illegal content accidentally.

Can you please specify why you do **not** agree with the statement: "A notice should make it **easy to identify** the alleged illegal content (for instance by providing a URL)"

N/a

Can you please specify why you do **not** agree with the statement: "A notice should **contain a detailed description of the alleged illegal nature of the content**"

N/a

Can you please specify why you do not agree with the statement: "A notice should contain evidence that the content provider could not be contacted before contacting the hosting service provider or

that the content provider was contacted first but did not act"

N/a

Both civil rights organisations and hosting service providers have complained about a significant proportion of unjustified or even abusive notices. Some stakeholders have proposed more effective sanctions and remedies for this purpose.

13.Should there be rules to avoid unjustified notifications? *

Yes

No

No opinion

Please explain:

Usually providers receive a substantial number of notices that are unjustified or not related to the providers' services, for instance notices coming from automated systems (such as spam), which cannot be reasonably processed. Therefore, Notice-and-Action regimes require the adoption of safeguards against such abuse and should be carefully developed to avoid unwarranted and unsubstantiated claims that hamper the free-flow of legitimate content. This is why notices should contain a series of details that allow for the identification of the sender, the identification of the content, its location, its alleged illegality, etc.

A set of minimum criteria would be helpful. These should correspond to the suggestions made in Q16. Some exceptions, notably regarding the necessity of contact details, might be needed for notifications by NGOs.

Safeguards should specifically address the case of third party complaints aimed at distorting competition, or aimed at substantive interruption of a legitimate firm's business.

Please explain:

14.How can unjustified notifications be best prevented? *

By requiring notice providers to give their contact details

By publishing (statistics on) notices

By providing for sanctions against abusive notices

Other

No action required

No opinion

Please specify:

In addition to the identification of the sender, which discourages against sending unjustified notices, safeguards might also include sanctions against notifications aimed at distorting competition, or aimed at substantive interruption of a legitimate firm's business. In the US, the DMCA provides for substantial penalties for false claims and requires notice providers to provide a statement on the accuracy of their notice as part of the minimum set of information required before filling a notice.

IV. Action against illegal content by hosting service providers

Hosting service providers, across Europe, react differently when they receive notice about content. For instance, some ensure a quick feedback to notice providers by sending a confirmation of receipt when they receive a notice and informing the notice provider when the requested action has been taken. Others do not. Similarly, some online intermediaries consult the provider of alleged illegal content whenever they receive a notice and offer the content providers the opportunity to give their views on the allegation of illegality concerning the content (the so-called "counter-notice"). Other providers do not consult the content provider.

15. Should hosting service providers provide feedback to notice providers about the status of their notice? *
Yes
<input checked="" type="checkbox"/> No
No opinion

<i>Multiple choice</i> *
<input checked="" type="checkbox"/> The hosting service provider should send a confirmation of receipt.
<input type="checkbox"/> The hosting service provider should inform the notice provider of any action that is taken.
<input type="checkbox"/> Other

Please explain:

Many hosting service providers already provide confirmation to the complainants about the receipt of their notice, if the senders' contact details are known. To what extent such practice should be established or maintained should be left to the hosting service providers' initiative and possibly in cooperation with authorities. Also, it is difficult to provide such a regime for all illegal activities and regarding all notices. In particular, notices coming from automated systems should not be followed up by any feedback from the providers. The promptness of hosting providers greatly depends on the complexity of the illegal content notified (eg child protection). A case by case approach is needed and we believe that self-regulation is the best tool to grant flexible and tailored rules.

Please explain:

16. Should hosting service providers consult the providers of alleged illegal content? *
--

Yes
<input checked="" type="checkbox"/> No
No opinion

<i>Multiple choice</i>
Upon receipt of a notice, but before any action as regards the alleged illegal content is taken. This would avoid the disabling / taking down of legal content.
Once any action against the content is taken. If it appears that the content was actually legal, it should be re-uploaded.
Other

Please specify:

There should be no obligation on providers to consult the alleged infringers. This responsibility should lie with the competent public authority in charge of assessing the alleged illegal content. If a consultation phase should be considered, the complainant must remain in charge of contacting the providers of alleged illegal content as a first step of the procedure. This preliminary step may have an important educational role.

Please specify:

According to the E-commerce Directive, the hosting provider should act "to remove or to disable access to the information"
- One may interpret "removing" as permanently taking down or deleting content.
- "Disabling access" can be understood as any technique that ensures that a user does not have access to the content. Some hosting service providers for instance use geo-software to impede access exclusively to users with an IP address from a country where the content in question is considered illegal. Similarly, some hosting service providers firstly impede access to all users without permanently deleting it. This can for instance allow law enforcement authorities to further analyse the alleged illegal content in the context of criminal investigations. If deleting would not any longer hinder the investigation, the hosting service provider may still remove the content.
17.Assuming that certain content is illegal, how should a hosting service provider act? *
The hosting service provider should remove the illegal content
The hosting service provider should first disable access to the illegal content
The hosting service provider should either remove or disable access. The sequence is not important.
<input checked="" type="checkbox"/> Other
No opinion

Please specify:

The Hosting Service Provider should in no case replace the role of the judicial authority in the assessment of the legality or illegality of the content or conduct. The HSP does not have a specific

technical competence nor the role to carry out such activity. Moreover, it would expose it to heavy risks of inappropriate or even illegal action by consumers. The hosting provider should first communicate the notice to the law Enforcement Authority (LEA) and act further only having been notified by the competent authority about its decision on the illegality of the content/conduct. Only after having received the LEA's decision, the provider may act in order to remove or disable (according to the said decision).

Several providers may host the same content on a particular website. For instance, a particular 'wall post' on the site of a social network may be hosted by the social network and by the hosting service provider that leases server capacity to the social network. It may be that this hosting service provider that leases server capacity is in a position to act against the alleged illegal content, but not without acting against other (legal) content.

18. When the same item of illegal content is hosted by several providers, which hosting service provider should act against it? *

The hosting service provider that is aware of the illegal content, but is not technically in a position to remove or disable only that illegal content and would for instance have to take down an entire site

The hosting service provider that is aware of the illegal content and is technically in a position to remove exclusively the notified illegal content

Other

No opinion

Please specify:

This would minimize the risk of removing "un-notified" legal content.

As soon as the illegal nature of certain content has been confirmed, the e-Commerce Directive requires the hosting service provider to act "*expeditiously*" if the provider is to be exempted from liability. However, the Directive does not further specify the concept of "expeditiously". Some stakeholders consider that a pre-defined timeframe for action should be established, whereas others consider that the required speed of action depends on the circumstances of the specific case. In a specific case it may be difficult to assess the legality of content (for instance in a case of defamation) or it may be easy to do so (for instance in a manifest case of child abuse content). This may have an impact on the speed of action. Similarly, what is expeditious for a specific category of content may not be sufficiently expeditious for another. For instance, the taking down of content within 6 hours will generally be considered very fast, but may not be sufficiently fast for the live-streaming of sports events (that are not any longer relevant once a match is finished).

19. Once a hosting service provider becomes aware of illegal content, how fast should it act? *

As fast as possible depending on the concrete circumstances of the case

Within a predefined time period

Other

Please specify:

The hosting service provider should only be required to act "expeditiously" after it has received confirmation from a LEA that the content is illegal. Before that, the notification in itself should not

be considered as a starting point for the “awareness” of the illegality, which can be considered as existing only after the legal assessment of a LEA. The term “expeditious” was carefully chosen to allow for the necessary flexibility (different national laws, different process depending on “category of illegal content etc) whilst ensuring legal certainty for hosting providers.

The confirmation should come from a competent authority. We fully agree with the Commission that “in specific cases it may be difficult to assess the legality of content (eg, in a case of defamation) or it may be easy to do so (eg, in a clear case of child abuse content). This may have an impact on the speed of action. Similarly, what is expeditious for a specific category of content may not be sufficiently expeditious for another. For instance, the taking down of content within 6 hours will generally be considered very fast, but may not be sufficiently fast for the live-streaming of sports events (that are not any longer relevant once a match is finished)”.

It has to be considered that the speed of removing content does not only depend on the hosting providers’ actions. The hosting provider needs confirmation from authorities about the content’s nature before taking any next step.

In individual cases, law enforcement authorities may ask hosting service providers not to act expeditiously on certain illegal content that are the subject of criminal investigations. Acting expeditiously could alert law infringers of the existence of a criminal investigation and would impede analysing the traffic on a particular site.

20. Should hosting service providers act expeditiously on illegal content, even when there is a request from law enforcement authorities not to do so? *

Yes

No

No opinion

Please explain:

Legal certainty is essential for hosting service providers. Hosting service providers must cooperate with public authorities and are obliged to execute the LEA’s orders. They are not in the position to make a choice between the interests protected by article 14 (private interests) and those protected by enforcement authorities for criminal investigations purposes (public interests).

Civil rights organisations complain that hosting service providers sometimes take down or disable access to *legal* content. They claim that some hosting service providers automatically act on notices without assessing the validity of the notices. In this context, the CJEU has held that blocking of legal content could potentially undermine the freedom of expression and information.

21. How can unjustified action against legal content be best addressed/prevented? *

By requiring detailed notices

By consulting the content provider before any action is taken

By providing easy and accessible appeal procedures

By publishing (statistics on) notices

By providing for sanctions against abusive notices

No action required

Other

No opinion

Please specify:

Legal certainty is essential for hosting service providers and therefore the risk of taking down or disabling access to a legal content should be reduced to the maximum extent possible.

The process of assessing the validity of the notification is crucial and should not be left in the hands of a private commercial organization. Hosting service providers may lack the full context and the expertise to judge whether particular content is illegal. The level of certainty for hosting service providers is aggravated by the fact that the same content can be deemed lawful or unlawful in different countries.

Incorrect assessment by hosting service providers may bear heavy consequences, not only in terms of their liability vis-à-vis their customers, but also in terms of a violation of fundamental rights such as the freedom of speech. This is particularly true in case of over-blocking.

Notification should be validated by a public authority (e.g. a court, Government appointed official or other independent third party) before a hosting service provider can be required to act on it.

Some hosting service providers are hesitant to take pro-active measures to prevent illegal content. They claim that taking such measures could be interpreted by courts as automatically leading to "actual knowledge" or "awareness" of all the content that they host. This would accordingly lead to a loss of the liability exemption they enjoy under the respective national implementation of the E-commerce Directive. In at least one national ruling, a court has interpreted actual knowledge in this sense. At the same time, the CJEU has held that awareness can result from own initiative investigations (Judgment of the Court of Justice of the European Union of 12 July 2011 in case C-324/09 (L'Oréal – eBay), points 121-122).

22. In your opinion, should hosting service providers be protected against liability that could result from taking pro-active measures? *
- Yes
 - No
 - No opinion

Since in the questionnaire the meaning of "pro-active measures" is not clearly explained, it would be appropriate for the Commission to clarify this for the sake of legal certainty. In the absence of such a precise definition, and in light of other pending Commission initiatives seeking to address the topic, we may generally consider in our reply below possible filtering mechanisms.

The general application of pro-active measures cannot be imposed by law: according to Article 15 of the e-Commerce Directive, Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14 (mere conduit, caching, hosting) to monitor the information which they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.

Any pro-active measures imposed on a HSP (i.e. a system for filtering) could in fact be interpreted as a general/automatic monitoring and therefore should be contrary to the provisions of the e-

Commerce Directive.

The adoption of such pro-active measures by hosting providers also raise concerns under a fundamental rights point of view since it may also infringe the fundamental rights of that hosting service provider's service users, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter of Fundamental Rights of the European Union respectively.

Some video platforms have already taken focused pro-active measures to prevent the posting of specific illegal content, such as the use of fingerprinting technology to filter uploaded videos. However, these voluntary efforts should not be interpreted as a basis for deciding that the intermediary has knowledge or control over the entire flow of data and they cannot be as basis in any way for the extension of an intermediary's liability. In any case, to be fully efficient the use of such technologies requires the involvement of all the stake-holders in the value chain, which, so far, has not happened.

Also, general pro-active measures may be a serious infringement of data privacy and could also bring into question issues around network neutrality.

Finally, the imposition or adoption of pro-active measures by providers would not pass the proportionality test. Imposing an excessive burden on providers would risk stifling innovative services and these measures are not 100% reliable.

Please explain:

V. The role of the EU in notice-and-action procedures

The E-commerce Directive encourages voluntary agreements on "rapid and reliable procedures for removing and disabling access" to illegal content. It also obliges the Commission to analyse the need for proposals concerning "notice-and-takedown" procedures.

23. Should the EU play a role in contributing to the functioning of N&A procedures? *

Yes

No

No opinion

Please specify :

By encouraging self-regulation

By providing non-binding guidelines

By providing some binding minimum rules

By providing binding detailed rules

A combination of these options

Other

Please explain:

The European Commission should encourage self-regulation as well as acknowledge existing efficient procedures, i.e. there should be a preference for the voluntary adoption and improvement of N&A mechanisms adapted to each specific illegal activity/content at stake as demonstrated by the existing mechanisms already implemented by providers to fight against illegal content. Guidelines may be helpful to ensure consistency between Member States where practices differ substantially and prove to be inefficient. These should set minimum criteria regarding the content of notices without jeopardizing business activities. Any effective guidance has to respect the national legislation.

Please specify:

Article 14 of the E-commerce Directive does not specify the illegal content to which it relates. Consequently, this article can be understood to apply horizontally to any kind of illegal content. In response to the public consultation on e-commerce of 2010, stakeholders indicated that they did not wish to make modifications in this regard.

24. Do you consider that different categories of illegal content require different policy approaches as regards notice-and-action procedures? *

Yes

No

Please clarify giving concrete examples relating to the question above:

As already mentioned, a horizontal approach would raise concerns given the huge differences that exist between different illegal activities carried out online and the associated social value and economic impact. There cannot be a one size fits all solution. Also, it has to be carefully considered that at European and national level, there are different legal frameworks already applicable to specific illegal activities, such as in the field of child protection (the recent European Directive) and illegal online gambling.

Keeping these national differences in mind, defining various policy actions for different kinds of illegal content should be proportionate to the severity of the rights at stake and balanced with the rights of other parties involved. Accordingly, child abuse material appears to be a particularly serious case of illegal content.

VI. Additional comments

If you have additional comments, you have the possibility to upload these in a separate document here. We would ask you to only use this option for comments you have not already expressed when answering the questions above.

25. Do you wish to upload a document with additional comments?
Yes
<input checked="" type="checkbox"/> No