COMMISSION RECOMMENDATION

of XX.2.2018

on measures to effectively tackle illegal content online

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

(1) [platform-positive agenda - special responsibility - voluntary actions/collaboration] Internet and service providers active on the Internet contribute significantly to innovation, economic growth and job creation in the Union. Many of those service providers play an essential role in the digital economy by connecting business and citizens and by facilitating public debate and the distribution and reception of factual information, opinions and ideas. However, their services are in certain cases abused by third parties to carry out illegal activities online, for instance disseminating certain information relating to terrorism, child sexual abuse, illegal hate speech or ~~infringements of intellectual property and~~ consumer protection laws, which can undermine the trust of their users and damage their business models. In certain cases the service providers concerned might even benefit from such activities, for instance as a consequence of the availability of copyright protected content without authorisation of the right holders, some providers have developed business mo

(2) The presence of illegal content also This ~~has s~~erious negative consequences for other ~~users~~, for other affected citizens and companies and for society at large. Online service providers therefore have particular responsibilities to help tackle illegal content disseminated through the use of their services. Many providers have therefore acknowledged and acted upon those responsibilities. At the collective level, important progress has been made through voluntary arrangements of various kinds, including in the context of the EU Internet Forum on terrorist content online since 2015, the Code of Conduct on Countering Illegal Hate Speech Online since May 2016 or the Memorandum of Understanding on the Sale of Counterfeit Goods singed in 2011 and revised in 2016. However, despite that commitment and progress, illegal content online remains a serious problem within the Union.

~~[voluntary actions/collaboration]~~ Many online ~~service providers have~~ear responsibilities ~~shown their commitment to tackle illegal content disseminated through the use of their services~~. T, ~~acknowledging that the presence of illegal content also undermines the trust of their users and damages their business models~~oviders h~~. At the col~~lective level, important progress has ~~been made through voluntary arrangements of various kinds, such as in the context of the Code of Conduct on Countering Illegal Hate Speech Online and the Memorandum of Understanding on the sale~~ of Ccounterfeit gGoods and the EU Internet

Forum. However, despite that commitment and progress, illegal content online remains a serious problem within the Union.

In particular, since its adoption in May 2016, the Code of Conduct on Countering Illegal Hate Speech has led to steady progress. Further progress should however still be made, in particular on transparency issues, including feedback to users. The Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet, first signed in 2011 and revised in 2016, has also led to measurable positive impacts. Further progress could nonetheless still be made, in particular in terms of wider participation and improved information exchange. [To be added: update on EU Internet Forum.]

(3) [Role of service providers] Those online service providers which mediate access to content for most internet users carry a significant societal responsibility in terms of protecting users and society at large and preventing criminals and other persons involved in infringing activities online from exploiting their services. In view of the evolution of their business models towards closer links between users and content and in view of technological developments, service providers are typically in possession of technical means to identify and remove illegal content.

(4) [Duty to act under existing legal framework] The service providers' duty to act, under certain circumstances, with a view to preventing or stopping illegal activities, is also recognised by Directive 2000/31/EC. This Directive further encourages the development of rapid and reliable procedures for removing or disabling access to illegal information and states that such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States.

(5) [What it means in concrete terms] Given that fast removal of illegal material is often essential in order to limit wider dissemination and harm, online platforms should be able to take swift decisions as regards possible actions with respect to illegal content online without being required to do so on the basis of a court order or administrative decision, especially where a law enforcement authority identifies and informs them of allegedly illegal content. At the same time, online platforms should put in place adequate safeguards when giving effect to their responsibilities in this regard, in order to guarantee users' rights of effective remedy. Online service providers should therefore have the necessary resources to understand the legal frameworks in which they operate.

(6) [calls for actions by other institutions, European Parliament, European Council] Concerned by series of terrorist attacks in the EU and proliferation of online terrorist propaganda, the European Council of 22-23 June 2017 stated that it "*expects industry to … develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts. This should be complemented by the relevant legislative measures at EU level, if necessary*". Similarly, the European Parliament, in its resolution on Online Platforms of June 2017, urged these platforms "*to strengthen measures to tackle illegal and harmful content*", while calling on the Commission to present proposals to address these issues. The call for the companies to take a more proactive approach in protecting their users from terrorist content has been reiterated by Ministers within the EU Internet Forum. In its Conclusions of 4 December 2014 on the enforcement of intellectual property rights, the Council stressed its commitment in the fight against intellectual property rights infringements while

safeguarding the fundamental rights of all parties concerned by intellectual property rights enforcement. It also called on the Commission to consider the use of tools available to identify intellectual property rights infringers and the role of intermediaries in assisting the fight against intellectual property rights infringements.

(7) [steps taken so far by the Commissions: Communication and pending proposals] On 28 September 2017, the Commission adopted a Communication with guidance on the responsibilities of online service providers in respect of illegal content online. In that Communication the Commission explained that it would assess whether additional measures are needed, *inter alia* by monitoring progress on the basis of voluntary arrangements. This Recommendation takes due account of and builds on the important progress made in that regard.

(8) This Recommendation acknowledges that due account should be taken of the particularities of the fight against different types of illegal content online and the specific responses that might be required, including through specific legislative measures, for instance in the field of copyright and the provision of audio-visual media servicesrmr the presence of illegal content, in the field of copyright. For instance, taking into acoutnition technologies for many years s have become main sources to consume protected content online, the Commission has adopted on 14 September 2016 a proposal for a directive on copyright in the digital single market that contains an obligation for those platforms to take measures aimed at preventing the upload of unauthorised content while, at the same time, facilitating the functioning of agreements between rights holders and platforms when such agreements exist. This obligation would be accompanied by safeguards for the users through the implementation of a redress mechanism which requires the collaboration from rights holders. This Recommendation leaves such legislative measures unaffected.

(9) [legal background: ECD] Directive 2000/31/EC of the European Parliament and of the Council[1] contains liability exemptions which are, subject to certain conditions, available to certain online service providers, including providers of 'hosting' services within the meaning of its Article 14. In order to benefit from that liability exemption, hosting service providers must act expeditiously to remove or disable access to illegal information that they store upon obtaining actual knowledge thereof and, as regards claims for damages, awareness of facts or circumstances from which the illegal activity or information is apparent. They can obtain such knowledge and awareness, inter alia, through notices submitted to them by one of the users of their services. As such, Directive 2000/31/EC constitutes the basis for the development of procedures for removing and disabling access to illegal information. That Directive also allows for the possibility for Member States of requiring the service providers concerned to apply a duty of care in respect of illegal content which they might store.

(10) When taking measures in respect of illegal content online, Member States are to respect the country of origin principle laid down in Directive 2000/31/EC. Accordingly, they may not, for reasons falling within the coordinated field as specified in that Directive, restrict the freedom to provide information society services by providers established in another Member State, subject however to the possibility of derogations under certain conditions set out in that Directive.

---

[1] [Reference.]

(11) [legal background: specific EU law] In addition, several other acts of Union law provide for a legal framework in respect of certain particular types of illegal content that are available and disseminated online. In particular, Directive 2011/93/EU of the European Parliament and of the Council[2] requires Member States to take measures to remove web pages containing or disseminating child pornography and allows them to block access to such web pages, subject to certain safeguards. Directive (EU) 2017/541 of the European Parliament and of the Council,[3] which is to be transposed into national law by 8 September 2018, contains similar provisions in respect of online content constituting public provocation to commit a terrorist offence. Directive 2017/541 also establishes minimum rules on the definition of criminal offences in the area of terrorist offences, offences related to a terrorist group and offences related to terrorist activities~~Directive (EU) 2017/541 also covers a number of other terrorist offences~~. Pursuant to Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights,[4] it ~~must be~~is possible for competent judicial authorities to issue injunctions against intermediaries whose services are being used by a third party to infringe an intellectual property right.

(12) [justification of N&A recommendations] In particular against this background, in addition to the voluntary measures taken by certain services providers, rules on so-called 'notice-and-action' mechanisms have been adopted by various Member States since the adoption of Directive 2000/31/EC. Other Member States consider adopting such rules. Such mechanisms generally seek to facilitate the notification of content which the notifying party considers to be illegal to the hosting service provider concerned ('notice'), pursuant to which that provider can decide whether or not it agrees with that assessment and wishes to remove or disable access to that content ('action'). However, the scope and content of that actual and potential future national legislation differs considerably. As a consequence, the service providers concerned can be subject to range of diverging legal requirements.

(13) [general aim] In the interest of the internal market and the effectiveness of the fight against illegal content online, as well as to safeguard the balanced approach that Directive 2000/31/EC seeks to ensure, it is necessary to set out certain main principles that should guide the activities of the Member States and the service providers concerned in this regard.

(14) [initial recital on fundamental rights, given their importance in the present context.] Those principles should be set out and applied bearing in mind that the fight against illegal content online must be carried out with proper and robust safeguards to ensure protection ~~often requires a fair balancing~~ of ~~several conflicting~~ the different fundamental rights at stake, notably those guaranteed in the Charter of Fundamental Rights of the European Union ('Charter'). In particular, ~~any~~ decisions taken by hosting service providers to remove or disable access to ~~illegal content, and any other~~ content in accordance with their terms of service under their contractual freedom, should take due account of the legitimate interests and rights of their users and of the central role which those providers tend to play in facilitating public debate and the distribution and reception of facts, opinions and ideas in accordance with the law.

---

2 [Reference.]
3 [Reference.]
4 [Reference.]

(15) -[scope - content] In accordance with the country of origin principle and the horizontal approach underlying the liability exemptions laid down in Directive 2000/31/EC, this Recommendation relates to any type of content which is not in compliance with Union law or with the laws of the Member State where the hosting service provider is established ~~and~~or, where that provider provides its services to users in other Member States and in as far as derogations from the country of origin principle apply, of the Member State where the services are provided, ~~, irrespective of the precise subject matter or nature of those laws.~~ It ~~therefore~~ covers in principle any type of illegal content online, irrespective of the precise subject matter or nature of those laws. However, when giving ~~a~~effect to the recommendations set out therein, due account should be taken of the relevant differences that might exist between various types of illegal content and the actions to be taken to tackle them.

(16) [scope – hosting service providers.] Providers of hosting services, such as, depending on the case, online market places and social media companies, play a particularly important role in tackling illegal content online, as they store information provided by and at the request of their users and give other users access thereto, often on a large scale. This Recommendation therefore primarily relates to the activities and responsibilities of those providers. Where appropriate, the recommendations laid down therein can however also be applied, *mutatis mutandis*, in relation to certain other providers of online services. As the purpose of this Recommendation is to address risks related to illegal content online affecting consumers in the Union, it relates to the activities of all such hosting service providers, regardless of whether they are established in the Union or in a third country, provided that they direct their activities to consumers residing in the Union.

(17) [general need for Notice and Action mechanism] Mechanisms for submitting notices regarding content which is considered to be illegal to hosting service providers are an important means to tackle illegal content online. Such mechanisms should facilitate the notification by all users who wish to do so. Therefore, those mechanisms should be easy to find and easy to use for all users. However, hosting service providers should have the necessary flexibility, for instance as regards the reporting format or technology that they use, so as to allow for efficient solutions and to avoid disproportionate burdens on those providers.

(18) [minimum requirements for notices] In accordance with the case law of the Court of Justice relating to Article 14 of Directive 2000/31/EC, notices should be sufficiently precise and adequately substantiated so as to allow the hosting service provider receiving them to take an informed and diligent decision as regards the effect to be given to the notice. It should therefore be ensured, as much as possible, that that standard is met. Whether or not a given notice leads to knowledge or awareness within the meaning of Article 14 of that Directive remains to be decided in light of the specificities of each individual case, however, bearing in mind that such knowledge or awareness can also be obtained through other means and that a notice made in accordance with tools provided by the service can provide such knowledge.

(19) [Contact details facultative] The inclusion of the contact details of the notice provider is generally not necessary for the hosting service provider to be able to take an informed decision as regards the effect to be given to the notice received. Requiring the provision of contact details as a precondition for being able to submit a notice may entail an obstacle to notification. However, the inclusion of the contact details is

necessary for the hosting service provider to be able to provide feedback. The inclusion of contact details should therefore be offered as a possibility for the notice provider, without this being an obligation, while explaining the consequences of not including any contact details.

(20) [Feedback to notice provider/content provider] In the interest of the accuracy of notice-and-action mechanisms and transparency and in order to allow for redress where needed, hosting service providers should, where they have the contact details of the persons involved, provide timely and adequate information to notice providers and to content providers regarding the steps taken as part of the operation of those mechanisms, in particular as regards their decisions on the requested removal or disabling access to the content concerned. The information to be provided should be proportionate in that it should correspond to the submissions made by the persons concerned~~,~~ in their notices or counter-notices, while allowing for differentiated and proportionate solutions and without imposing an excessive burden on the providers.

(21) [counter-notice and exceptions] Allowing content providers an opportunity to challenge the decision of the hosting service provider to remove or disable access to content stored at his or her request, regardless of whether that decision was taken after the reception of a notice or a referral or pursuant to proactive measures, generally contributes to achieving ~~is an important safeguard to ensure~~ transparency and fairness and to ~~to~~ avoiding the unintended removal of content which is not illegal.

(22) However, informing the content provider and allowing him or her an opportunity to submit a counter-notice might in certain cases involve a serious and objective risk of disrupting criminal investigations which outweighs the interest of the content provider in being informed and able to exercise that opportunity immediately. Where a competent authority so requests, hosting service providers should therefore refrain from informing the content provider of the decision to remove or disable access and from giving him the opportunity to challenge that decision, for as long the competent authority deems that necessary in light of that risk. In as far as this entails a restriction of the right to be informed in respect of the processing of personal data, the relevant conditions set out in Regulation (EU) No 2016/679 should be complied with.

(23) [judicial review untouched + out-of-court settlement] Notice-and-action mechanisms should not in any way affect the rights of the parties involved to initiate legal proceedings, in accordance with the applicable law, in respect of any content which is considered to be illegal or of any measures taken in this regard by hosting service providers. Mechanisms for the settlement, out-of-court, of disputes arising in this connection can be an important complement to judicial proceedings, especially where they allow for the effective, cheap and swift resolution of those disputes. Such out-of-court settlements should therefore be encouraged, provided that the relevant mechanisms meet certain standards and the parties' access to court remains unaffected and that these mechanisms are not used with the objective of impeding the tackling of illegal content.

(24) [transparency requirements] Transparency vis-à-vis the general public regarding the functioning of notice-and-action mechanisms and other activities of hosting service providers in respect of illegal content and other content which they might remove or to which they disable access is an important means to determine the effectiveness of those mechanisms and other activities. It is also an important safeguard, in particular

as regards the possible removal of or disabling of access to content which is not illegal but which might be against the service provider's terms of service. Hosting services providers should therefore regularly publish reports which are sufficiently complete and detailed to allow for an adequate insight into their activities. They should also provide for clarity *ex ante*, in their terms of service, on their policies in this regard.

(25) [pro-active measures & "Good Samaritan clause"] In addition to notice-and-action mechanisms, proportionate and specific proactive measures taken voluntarily by hosting service providers, including by using automated means in certain cases to detect and possibly suspend access to it, can also be an important element in tackling illegal content online. Whether it is appropriate to take such measures can depend, *inter alia*, on the nature, scale and purpose of those measures, the type of content at issue, whether it has been notified by law enforcement authorities, whether action had already been taken in respect of the content and the need to assess the relevant context in order to determine whether or not the content is to be considered illegal content. Action should be taken to support~~Account should also be taken of~~ the generally more limited resources and expertise of smaller hosting service providers and account should be taken of~~,~~ the need for sufficient~~adequate and effective~~ safeguards accompanying such measures, as well as the prohibition for Member States to impose a general monitoring obligation or an obligation to actively seek for facts or circumstances indicating illegal activity set out in Article 15(1) of Directive 2000/31/EC.

(26) In this context, the Commission's Communication of 28 September 2017 on tackling illegal content online also recalled that proactive measures taken by those online platforms which fall under Article 14 of Directive 2000/31/EC to detect and remove illegal content which they host – including the use of automatic tools and tools meant to ensure that previously removed content is not re-uploaded - do not in and of themselves lead to a loss of the liability exemption.

(27) [safeguards] It is essential that any measures taken to tackle illegal content online are subject to proper and robust safeguards and that hosting service providers act diligently when setting and enforcing their policies in respect of any content that they store, including illegal content, so as to ensure, in particular, that users can freely receive and impart information online in compliance with the applicable law. Particular safeguards, notably human oversight and verifications~~ where appropriate~~, should be provided for where appropriate in relation to the use of automated means, so as to avoid any unintended and erroneous decisions. Those safeguards should be provided for and applied in addition to any specific safeguards laid down in the applicable law, for instance regarding the protection of personal data.

(28) [cooperation: Member States and providers] Smooth, effective and appropriate cooperation between competent authorities and hosting service providers in the fight against illegal content online should be ensured. To that aim, they should designate points of contacts and procedures should be established for the processing of notices submitted by those authorities as a matter of priority and with an appropriate degree of confidence as regards their accuracy, taking account of the particular responsibilities and expertise of those authorities. In order to effectively tackle the most serious offences of which hosting service providers might become aware when carrying out their activities, namely those constituting criminal offences under the laws of the Member States, Member States should be encouraged to make use of the possibility

set out in Article 15(2) of Directive 2000/31/EC to establish in law reporting obligations, in compliance with the applicable law, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council[5].

(29) [trusted flaggers] In addition to competent authorities, certain individuals ~~or~~, entities, ~~including~~ non-governmental organisations or other users~~;~~ might take on, on a voluntary basis, certain responsibilities in the fight against illegal content online and might also have particular expertise. Where it is ensured that they act diligently and in a responsible manner, as well as in full respect of fundamental rights and of democratic values, they should therefore be considered as trusted flaggers and they should be involved in that fight, in particular by treating the notices that they submit also a matter of priority and with an appropriate degree of confidence as regards their accuracy.

(30) [cooperation: between providers / situation of smaller companies, SMEs] Combating illegal content online requires a holistic industry approach, as illegal content often easily migrates from one hosting service provider to another and tends to exploit the weakest links in the chain. Cooperation, consisting in particular of the sharing on a voluntary basis of experiences, technological solutions and best practices, is therefore essential. This is ~~P~~particular important in view of~~attention should be paid~~ to the position and typically more limited resources and expertise of smaller hosting service providers.

(31) [explanation of the particularity of terrorist content] Terrorist activities entail particularly grave risks to ~~Union~~ citizens and ~~its~~ society at large, in particular to human life. The Internet, and the use made of certain hosting services, have moreover been shown to play a key role in disseminating terrorist content, often by persons and groups operating on a professional scale, thus significantly increasing those risks. At the EU Internet Forum whilst progress has been achieved, there remains an urgent need for a swifter response to terrorist content online. This includes the greater use of technology developed by the platforms to identify and remove terrorist content, as well as to prevent its dissemination and re-uploading, to support small companies enhance their resilience to terrorists' exploitation, and to improve the transparency of reporting and cooperation with competent authorities. In light of th~~ose~~ particularities related to tackling terrorist content online, ~~and considering that Member States are now to take measures for the removal of or disabling of access to certain types of terrorist content pursuant to Directive (EU) 2017/541,~~ the recommendations relating to tackling illegal content generally should be complemented by certain recommendations which specifically relate to the fight against terrorist content online, building on and consolidating efforts undertaken in the framework of the EU Internet Forum.

(32) [general] Considering th~~ose~~ particularly grave risks associated with terrorist content and hosting service providers' ~~their~~ central role in the dissemination of such content, they~~hosting service providers~~ should ~~be encouraged~~ not ~~to~~ tolerate any terrorist content among the information that they store and to take all reasonabl~~y~~e measures to tackle terrorist content, subject to their possibility to set and enforce their terms of service and the need for effective and adequate safeguards and without prejudice to Article 14 of Directive 2000/31/EC.

5

(33) [referrals] Those measures should, in particular, consist of cooperating with competent authorities and Europol through referral mechanisms, as a specific means for notifying hosting services providers which is adapted to the particularities of the fight against terrorist content. When submitting referrals, competent authorities and Europol should be able to request the removal or disabling of access to content which they consider to be terrorist content either with reference to the relevant applicable laws or to the terms of service of the hosting service provider concerned. Those referral mechanisms should exist ~~and content related to terrorism which is precluded by the terms of service of hosting service providers.~~ in addition to the mechanisms for submitting notices, including by trusted flaggers, which may also be used for notifying terrorist content.

(34) [fast removal] Given that the potential harm caused by terrorist content tends to increase exponentially in function of the time it remains online, the fact that terrorist content is most harmful in the first hours of its appearance online and the specific responsibilities and expertise of competent authorities and Europol, referrals should be assessed and, where appropriate, acted upon within one hour, except in duly justified cases where this is not technically feasible ~~in a particularly expeditious manner~~.

(35) [proactive measures] Those measures to tackle terrorist content should also consist of proportionate and specific proactive measures, including by using automated means, in order to detect, identify and expeditiously remove or disable access to terrorist content and to ensure that terrorist content does not reappear, without prejudice to Article 15(1) of Directive 2000/31/EC. For practical and operational reasons, notwithstanding cooperation measures between hosting providers, account should also be taken of the generally more limited resources and expertise of smaller hosting service providers, the need for adequate and effective safeguards accompanying such measures, as well as the prohibition to impose a general monitoring obligation or an obligation to actively seek for facts or circumstances indicating illegal activity set out in Article 15(1) of Directive 2000/31/EC.

(36) [cooperation] Cooperation, both between hosting service providers and with competent authorities, is of the utmost importance when seeking to tackle terrorist content. In particular, technological tools that allow for automated content detection ~~recognition~~, such as the database of hashes, can help achieve the objective of preventing the dissemination of content considered to be terrorist content across different hosting services. The development, ~~and~~ operation and cross-industry sharing of such tools on a cooperative basis by hosting services providers should therefore be encouraged. The conclusion of working arrangements between all relevant parties, including where appropriate Europol, should also be encouraged, as such arrangements can help ensure a consistent and effective approach and allow for the exchange of relevant experiences and expertise.

(37) [general recital in data protection] In order to ensure respect for the fundamental right to the protection of natural persons in relation to the processing of personal data, as well as the free movement of personal data, the processing of personal data in the context of any measures taken to give effect to this Recommendation should be in full compliance with the rules on data protection, in particular with Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council[6], and should be the monitored by the competent supervisory authorities.

---

[6] [Reference.]

(38) [charter recital (general)] Respect for the fundamental rights protected in the Union's legal order of all parties concerned is of particular importance when addressing the challenges associated with tackling illegal content online. In addition to right to protection of personal data, those rights include, as the case may be, the freedom of expression and information and the rights to protection of privacy and effective judicial protection of the users of the services concerned. They may also include the freedom to conduct a business, including the freedom of contract, of hosting service providers, as well as the rights of the child and the rights to protection of property, including intellectual property, to human dignity and to non-discrimination of certain other affected parties.

(39) This Recommendation respects the fundamental rights and observes the principles recognised in particular by the Charter. In particular, this Recommendation seeks to ensure full respect for Articles 1, 7, 8, 10, 11, 16, 17, 21, 24 and 47 of the Charter.

(40) [monitoring and possible next steps] ~~It is important that the Commission is in a position to adequately assess the effects given to this Recommendation.~~The Commission intends to closely monitor the actions taken in response to this Recommendation. Member States and hosting service providers should therefore ~~be~~ regularly submit ~~prepared to provide~~ to the Commission ~~with~~ all the relevant information ~~which they can reasonably be expected to provide~~ in order to allow this monitoring ~~for such an adequate assessment,~~ upon request by the Commission for illegal content in general and regularly, without such request, for terrorist content. On the basis of that information and all other available information, including reporting on the basis of the various voluntary arrangements, the Commission will assess those effects, at the latest ~~three~~ six months from the date of the publication of this Recommendation, and determine whether additional steps, including proposing binding acts of Union law, are required.

HAS ADOPTED THIS RECOMMENDATION:

CHAPTER I

PURPOSE AND TERMINOLOGY

1. Member States and hosting service providers, in respect of content provided by content providers which they store, are encouraged to take effective, appropriate and proportionate measures to tackle illegal content online, in accordance with the principles set out in this Recommendation and in full compliance with the Charter and other applicable provisions of Union law, in particular as regards the protection of personal data, competition and electronic commerce.

2. This Recommendation takes due account of and builds on voluntary arrangements agreed between hosting service providers and other affected service providers regarding different types of illegal content. In the area of terrorism, it builds on and consolidates, in particular, the progress made in the framework of the EU Internet Forum.

3. This Recommendation is without prejudice to the rights and obligations of Member States to take measures in respect of illegal content online in accordance with Union law, including the possibility for courts or administrative authorities of Member

States, in accordance with their respective legal systems, of requiring hosting service providers to remove or disable access to illegal content. This Recommendation is also without prejudice to the position of hosting service providers under Directive 2000/31/EC and the possibility for hosting service providers to set and enforce their terms of service in accordance with Union law and the laws of the Member States.

4. For the purpose of this Recommendation, the following terms are used:

(a) 'hosting service provider' means a provider of information society services consisting of the storage of information provided by the recipient of the service at his or her request, within the meaning of Article 14 of Directive 2000/31/EC, irrespective of its place of establishment, which directs its activities to consumers residing in the Union;

(b) 'illegal content' means any information which is not in compliance with Union law or the laws of the Member State in which the hosting service provider concerned is established ~~and~~or, as the case may be, of the Member State where it provides its services, irrespective of the nature or specific subject matter of those laws;

(c) 'user' means any natural or legal person who is the recipient of the services provided by a hosting service provider;

(d) 'content provider' means a user who has submitted information that is, or that has been, stored at his or her request by a hosting service provider;

(e) 'notice' means any communication addressed to a hosting service provider submitted by a notice provider in respect of content stored by that hosting service provider which the notice provider considers to be illegal content, requesting the removal of or the disabling of access to that content by that hosting service provider ~~on a voluntary basis~~;

(f) 'notice provider' means a user who has submitted a notice to a hosting service provider;

(g) 'trusted flagger' means a user which is deemed by a hosting service provider to have particular responsibilities and expertise for the purpose of tackling illegal content online;

(h) 'terrorist content' means any information the dissemination of which amounts to offences specified in Directive (EU) 2017/541 or terrorist offences specified in the laws of the Member State in which the hosting service provider concerned is established or, as the case may be, of the Member State where it provides its service~~s~~, including the dissemination of relevant information produced by or attributable to or in support of? terrorist groups or entities included ~~an organisation listed o~~in the relevant lists ~~of terrorist organisations~~ established by the Union or by the United Nations;

(i) 'law enforcement authorities' means the competent authorities designated by the Member States in accordance with their national laws to carry out law enforcement tasks for the purposes of the prevention, investigation,

detection or prosecution of criminal offences in connection to illegal content online;

(j) 'competent authorities' means the competent authorities designated by the Member States in accordance with their national laws to carry out tasks which include tackling illegal content online, including law enforcement authorities and administrative authorities charged with enforcing laws, irrespective of the nature or specific subject matter of those laws, applicable in certain particular fields;

(k) 'referral' means any communication addressed to a hosting service provider submitted by a competent authority or by Europol in respect of content stored by that hosting service provider which that authority or Europol considers to be ~~either~~ terrorist content ~~or content related to terrorism which is precluded by the terms of service of that hosting service provider~~, requesting the removal of or the disabling of access to that content by that hosting service provider on a voluntary basis.

CHAPTER II

GENERAL RECOMMENDATIONS RELATING TO ALL TYPES OF ILLEGAL CONTENT

Mechanisms for submitting and processing notices

5. Provision should be made for mechanisms allowing any user to submit notices to hosting service providers in respect of any content that those providers store. Those mechanisms should be easy to find, user-friendly and allow for the submission of notices by electronic means.

6. The mechanisms for submitting notices should allow for and encourage the submission of notices which are sufficiently precise and adequately substantiated to enable the hosting provider concerned to take an informed decision in respect of the content to which the notice relates, in particular whether or not that content is to be considered illegal content and is be removed or access thereto is be disabled. ~~To that aim, notices should, in particular, contain an explanation of the grounds on which the content is considered illegal content and a clear indication of the exact location of the content.~~Those mechanisms should be such as to facilitate the provision of notices that contain an explanation of the reasons why the notice provider considers the content concerned to be illegal content and a clear indication of the location of that content.

7. Notice providers should have the opportunity, but not be required, to include their contact details in a notice. Where they decide to include their contact details, their anonymity should be ensured towards the content provider, without prejudice to any applicable legal obligations for hosting service providers to provide certain information to competent authorities.

8. Where the contact details of the notice provider are known to the hosting service provider, the hosting service provider should send a confirmation of receipt to the notice provider and should, without undue delay, inform in a proportionate manner the notice provider of its decision in respect of the content to which the notice relates.

Counter-notices and information of content provider

9. Where a hosting service provider decides to remove or disable access to any content that it stores because it considers the content to be illegal content, including by means of automated detection technologies, and where the contactent details of the content provider are known to the hosting service provider, the content provider should, without undue delay, be informed of that decision and of the reasons for taking it.

10. In the situation referred to in point 9, the content provider should be given the possibility to contest the decision by the hosting service provider within a reasonable time period, through the submission of a counter-notice to the hosting service provider concerned. The content provider should be informed of that possibility. The mechanism to submit such counter-notices should be user-friendly and allow for submission by electronic means.

11. However, there should be no provision of the information referred to in points 9 and 10 where a competent authority has informed the hosting service provider concerned that the provision of that information would interfere with the exercise of its investigative powers relating to criminal offencesof, and for as long as, a competent authority of a Member State requests the hosting service provider not to provide such information for reasons of public policy and public security and in particular the prevention, investigation, detection and prosecution of criminal offences.

12. It should be ensured that hosting service providers take due account of any counter-notice that they receive. Where the counter-notice has provided reasonable grounds leadings the hosting service provider to consider that the content to which the counter-notice relates is not to be considered illegal content, it should reverse its decision to remove or disable access to that content without undue delay, without prejudice to its possibility to set and enforce its terms of service in accordance with Union law and the laws of the Member States.

13. The content provider who submitted a counter-notice, as well as the notice provider concerned, should, where their contact details are known to the hosting service provider concerned, be informed, without undue delay, of the decision that the hosting service provider has taken in respect of the content concerned.

Out-of-court dispute settlement

14. Member States are encouraged to facilitate, where appropriate, out-of-court settlements to resolve disputes related to the removal of or disabling of access to illegal content. Any mechanisms for such out-of-court dispute settlement should be easily accessible, effective, transparent and impartial and should ensure that the settlements are fair and in compliance with the applicable law. Attempts to settle

such disputes out-of-court should not affect the access to court of the parties concerned.

15. Where available in the Member State concerned, hosting service providers are encouraged to allow the use of out-of-court dispute settlement mechanisms.

Transparency

16. Hosting service providers ~~should~~ should be be ~~en~~couraged to publish clear, easily understandable and sufficiently detailed explanations of their policy in respect of the removal or disabling of access to any ~~con~~tent that they store, including content considered to be illegal content.

17. Hosting service providers ~~should~~ should be ~~be~~ encouraged to publish at regular intervals, preferably at least annually, reports on their activities relating to the removal and the disabling of ~~access to any content that they store, including content considered to be~~ illegal content. Those reports should include, in particular, information on the amount and type of content removed, on the number of notices and counter-notices received and the time needed for taking action.

Proactive measures

18. Hosting service providers should be encouraged to take, where appropriate, proportionate and specific proactive measures in respect of illegal content. Such proactive measures could involve the use of automated means for the detection of illegal content only where appropriate and proportionate and subject to adequate and effective safeguards, in particular the safeguards referred to in points 19 and 20.

Safeguards

19. In order to avoid removal of content which is not illegal content, without prejudice to the possibility for hosting service providers to set and enforce their terms of service in accordance with Union law and the laws of the Member States, there should be effective and appropriate safeguards to ensure that hosting service providers act diligently in respect of any content that they store, in particular when processing notices and counter-notices and when deciding on the possible removal of or disabling of access to content considered to be illegal content.

20. Where hosting service providers use automated means in respect of any content that they store, adequate safeguards should be provided for to ensure that ~~any~~ decisions taken concerning that content involving the use of those means, in particular decisions to remove or disable access to content considered to be illegal content, are accurate and well-founded. Such safeguards should consist, in particular, of human oversight and verifications, where appropriate. They should where appropriate ~~and in any case~~t of human oversight and verifications where a detailed assessment of the relevant context is required in order to determine whether or not the content is to be considered illegal content.

Protection against abusive behaviour

21. Effective and appropriate measures should be taken to prevent the submission of, or the taking of action upon, notices or counter-notices that are submitted in bad faith and other forms of abusive behaviour related to the recommended measures to tackle illegal content online set out in this Recommendation.

Cooperation between hosting services providers and Member States

22. Member States and hosting service providers should designate points of contact for matters relating to illegal content online..

23. Fast-track procedures should be provided for to process notices submitted by competent authorities.

24. Member States are encouraged to establish legal obligations for hosting service providers to promptly inform law enforcement authorities, for the purposes of the prevention, investigation, detection or prosecution of criminal offences, of any evidence of alleged serious criminal offences where there is a threat to the life or safety of persons at stake obtained in the context of their activities for the removal or disabling of access to illegal content, in compliance with the applicable legal requirements, in particular regarding the protection of personal data protection, including Regulation (EU) 2016/679.

Cooperation between hosting services providers and trusted flaggers

25. Hosting service providers should be encouraged to publish clear and objective conditions to determine which users they consider as trusted flaggers. ~~consider as trusted flagger individuals and entities which meet appropriate conditions to ensure that they carry out their activities as trusted flaggers in a diligent and responsible manner.~~ Those conditions~~criteria~~ should aim to ensure that trusted flaggers act in a diligent, responsible, independent and objective manner, based on respect for fundamental rights and of democratic values, and~~, in particular, ensure that those individuals or entities~~ have the necessary expertise ~~and carry out those activities as accurately and effectively as possible, in good faith and in an independent and impartial manner~~. ~~Those criteria should be published.~~

26. oe criteria without further assessment by the hosting servic

27. Cooperation between hosting service providers and trusted flaggers should be encouraged. In particular, fast-track procedures should be provided for to process notices submitted by trusted flaggers.

Cooperation between hosting service providers

28. Hosting service providers should, where appropriate, share experiences, technological solutions and best practices to tackle illegal content online among each other and in particular with hosting service providers which, because of their size or the scale on which they operate, have limited resources and expertise, including in the context of ongoing cooperation between hosting service providers through codes of conduct, memoranda of understanding and other voluntary arrangements.

CHAPTER III

SPECIFIC RECOMMENDATIONS RELATING TO TERRORIST CONTENT

29. The recommendations set out in this Chapter apply in addition to the recommendations set out in Chapter III.

Recommended ~~G~~general measures

30. Hosting service providers should expressly set out in their terms of service that they will not store terrorist content.

31. ~~H~~Hosting service providers should take ~~all necessary~~ measures so that ~~to ensure that~~ they do not store terrorist content, in particular in relation to the processing of and swift response to notices, referrals, ~~tproactive measures and as regards cooperation i~~n accordance ~~w~~with the following points~~, subject~~ to adequate and effective safeguards and in particu~~lar the safeguards referred to in points 19 and 20.~~

Mechanisms for submitting and processing referrals

32. Member States should ensure that their competent authorities have the capability and sufficient resources to effectively detect and identify terrorist content and to submit referrals to the hosting service providers concerned, in particular through national internet referral units and in cooperation with the EU Internet referral unit of Europol.

33. P~~p~~Provision should be made for mechanisms allowing for ~~the~~ submission of referrals. Fast-track procedures should be provided ~~for~~ to process referrals, in particular referrals submitted by national internet referral units and by the EU Internet referral unit of Europol.

34. Hosting service providers should, without undue delay, send confirmations of receipt of referrals and inform the competent authority or Europol of their decisions in respect of the content to which the referrals relate. They should indicate when the content was removed or access thereto was disabled or, as the case may be, ~~,~~ explain why they ~~providing explanations where the hosting service provider~~ decided not to remove or to disable access to th~~a~~e content.

35. Hosting service providers should assess and, where appropriate, remove or disable access to content identified in referrals, as a general rule, within one~~two~~ hours from the moment at which they received the referral.

36. Member States should participate in the EU referral platform established by Europol. Hosting service providers should use that e EU referral platform as a central repository of terr

Proactive measures

37. Hosting service providers should ~~be encouraged to~~ take proportionate and specific proactive measures, including by using automated means, in order to detect, identify and immediately ~~expeditiously~~ remove or disable access to terrorist content.

38. Hosting service providers should ~~be encouraged to~~ immediately take proportionate and specific proactive measures, including by using automated means, in order to prevent content providers from re-submitting content which has already been removed or to which access has already been disabled because it is considered to be ~~illegal~~ terrorist content.

Cooperation

39. In order to prevent the dissemination of content considered to be terrorist content across different hosting services, hosting service providers should be encouraged to cooperate through the sharing and optimisation of effective, appropriate and proportionate technological tools, including such tools that allow for automated content recognition. Where technologically possible, all relevant formats through which terrorist content is disseminated should be captured. Such cooperation should include, in particular, hosting service providers which, because of their size or the scale on which they operate, have limited resources and expertise.

40. Hosting service providers should be encouraged to take the necessary measures for the proper functioning and improvement of the tools referred to in point 36, in particular by providing identifiers relating to all content considered to be terrorist content and by fully exploiting the possibilities of those tools.

41. Competent authorities and hosting service providers should conclude working arrangements, where appropriate also with Europol, on matters relating to terrorist content online, including for enhancing the understanding of terrorist activities online, improving referral mechanisms and facilitating requests by law enforcement authorities for the purposes of criminal investigations in relation to terrorism.

Reporting on referrals

42. ~~Hosting service providers particularly exposed to terrorist content on their platforms should report every three months on the implementation of the above recommendations. Such reports should in particular cover the amount and speed of terrorist content removed in total, and how much content has been prevented from being uploaded, through the use of automation and technological tools such as the database of hashes. Reporting on such tools should cover how many pieces of content it includes, broken down by format/content type as well as by source. Reporting on law enforcement notices/referrals should cover number of notices/referrals received, success rate of removals as well as speed of removals.~~

43. Member States should, every three months, report to the Commission ~~every three months~~ on the referrals submitted by their competent authorities and the decisions taken by hosting service providers upon those referrals, as well as on their cooperation with hosting service provider relating to tackling terrorist content online.

CHAPTER IV

MONITORING AND PROVISION OF INFORMATION

44. In order to allow for the monitoring of the effects given to this Recommendation as regards illegal content, other than terrorist content, at the latest ~~three~~ six months from the date of its publication, , Member States and hosting service providers should submit to the Commission, at its request, all the relevant information to allow for such monitoringMember States and hosting servi~~ce~~ providers should take the necessary measures to be able to provide relevant information to the ~~Comm~~ission.

45. In order to allow for the monitoring of the effects given to this Recommendation as regards terrorist content at the latest three months from the date of its publication, … As far as terrorist content is concerned, the reports should cover, in particular, the amount and speed of terrorist content removed in total and how much content has been prevented from being uploaded, through the use of automation and technological tools. Reporting on such tools should cover how many pieces of content it includes, broken down by format/content type as well as by source. Reporting on law enforcement notices/referrals should cover number of notices/referrals received, success rate of removals as well as speed of removals.

Done at Brussels, XX.2.2018

For the Commission
XYZ
[title]… of the Commission