DEFENDING FREEDOM
OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org

ARTICLE 19

Internet intermediaries: Dilemma of Liability

ARTICLE 19
Free Word Centre
60 Farringdon Road
London
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

ISBN: 978-1-906586-61-4

This document has been published with support of the Adessium Foundation of The Netherlands, as part of their wider support for ARTICLE 19's work on freedom of expression and internet communications technology.

Contents

Executive summary

Internet intermediaries – such as internet service providers, search engines and social media platforms – play a crucial role in enabling people around the world to communicate with each other. Because of their technical capabilities, internet intermediaries are under increasing pressure from governments and interest groups to police online content.

At the same time, various intermediaries ban certain types of content, usually outside the scope of any internationally-recognised legitimate limitations on freedom of expression. The problem is further compounded by the lack of transparency in the way these limitations are implemented, the lack of clear guidelines to which users could refer, and the absence of appropriate mechanisms which can be used to appeal against any decisions made by the internet service providers (ISP), all of which amount to the censorship of user-generated content. This effectively means that online content is increasingly being regulated and censored via private contracts which offer limited transparency and accountability.

Responding to this situation, this policy document focuses on various aspects of intermediaries' liability. Drawing upon international freedom of expression standards and comparative law, it explains the risks that the currently widespread regime of liability poses to the exercise of freedom of expression online. It proposes a number of alternative models which can already be found in some jurisdictions and which offer stronger protection to online freedom of expression.

We hope that this policy brief will help legislators, policy makers, judges and other stakeholders strike the right balance between, on the one hand, the protection of freedom of expression online and, on the other hand, the protection of other interests, such as the prevention of crime and the rights of others.

Key recommendations

- Web hosting providers or hosts should in principle be immune from liability for third-party content when they have not been involved in modifying the content in question.
- Privatised enforcement mechanisms should be abolished. Hosts should only be required to remove content following an order issued by an independent and impartial court or other adjudicatory body which has determined that the material at issue is unlawful. From the hosts' perspective, orders issued by independent and impartial bodies provide a much greater degree of legal certainty.
- Notice-to-notice procedures should be developed as an alternative to notice and take down procedures. These would allow aggrieved parties to send a notice of complaint to the host. Notice-to-notice systems should meet a minimum set of requirements, including conditions about the content of the notice and clear procedural guidelines that intermediaries should follow.
- Clear conditions should be set for content removal in cases of alleged serious criminality.

Introduction

It is estimated that there are now over 7 billion people connected to the internet. Internet intermediaries – a broad term which includes web hosting companies, Internet Service Providers (ISPs), search engines and social media platforms[1] - play a crucial role in enabling people to access the internet and in transmitting third-party content.

Without ISPs, there would be no access to the internet and to the wealth of information that we have become accustomed to being able to access at the click of a mouse. Without social media and blogging platforms, ordinary internet users would lose a valuable way of publishing their opinions and instantaneously sharing information.

Originally, intermediaries were generally subject to limited regulation, especially in Western countries where the internet was commercialised in the 1990s.[2] However, in recent years, there has been increasing pressure on internet intermediaries to act as 'gatekeepers' of the internet. Using a variety of means, a growing number of governments have started to enlist - or in some cases compel - intermediaries to remove or block their citizens' access to content which they deem illegal or "harmful."[3] While some of these restrictions are applied directly by a state regulator,[4] many states have adopted legal regimes for civil liability that have effectively forced internet intermediaries to police aspects of the internet on the state's behalf.[5]

This kind of pressure is not limited to Internet Service Providers and social media platforms; it can also be targeted at advertisers and at electronic payment systems such as Paypal. By exercising political or legal pressure and threatening and damaging their revenue streams online, governments can very effectively censor organisations which defend causes that they don't like.[6]

Meanwhile, under their terms and conditions, various intermediaries (in particular social media platforms and electronic payment systems[7]) ban certain types of content (e.g. nudity or information about reproductive rights services), usually outside the scope of any internationally-recognised legitimate limitations on freedom of expression. The problem is further compounded by the lack of transparency in the way in which these limitations are implemented, the lack of clear guidelines to which users can refer, and the absence of appropriate mechanisms to appeal against any decisions made by the ISP, all of which amount to the censorship of user-generated content. This effectively means that online content is increasingly being regulated and censored via private contracts which offer limited transparency and accountability.

All of the above create an incredibly complex regulatory environment, in which internet users' rights, including the right to freedom of expression and the rights to privacy and access to information, are easily subject to abuse.

In response to this complicated situation, ARTICLE 19 is issuing the first of two position briefs about online content regulation. This brief focuses on intermediaries' liability.[8] It seeks to explain the risks posed by the currently widespread regime of liability to the exercise of freedom of expression online. It proposes a number of alternative models which can be found in some jurisdictions and which offer stronger protection to online freedom.

We hope that this brief will offer clear answers to the question of how to strike the right balance between the protection of the right to freedom of expression and the protection of other interests, such as the prevention of crime and the rights of others.

Internet intermediaries: basic facts

Types of intermediaries

Given the complexity of the internet, there are a number of different types of intermediaries. For the purposes of this paper, the most relevant are internet service providers (ISPs), web hosting providers, social media platforms and search engines:

- Internet Service Providers (ISPs): this term can be confusing because it is commonly used to describe both access providers (those who control the physical infrastructure needed to access the internet, who typically make this infrastructure available to individual subscribers in return for payment) and hosts. In this brief, the term ISPs is used to refer only to access providers.
- Web hosting providers or 'hosts': hosts are bodies (typically companies) that rent web server space to enable their customers to set up their own websites. However, the term 'host' has also taken on a more general meaning, i.e. any person or company who controls a website or a webpage which allows third parties to upload or post material. For this reason, social media platforms, blog owners, and video- and photo-sharing services are usually referred to as 'hosts'.
- Social media platforms: the distinctive feature of social media platforms (such as Facebook or Twitter) is that they encourage individuals to connect and interact with other users and to share content. Another name for them is 'web 2.0 applications'. They are usually considered to be 'hosts' because they allow third parties to post content. This is important since, in some countries, the liability regime is different depending on whether or not a company (or other body) is regarded as a hosting provider or as an access provider.
- Search engines are software programmes that use sophisticated algorithms to retrieve data, files or documents from a database or network in response to a query. The information retrieved is usually indexed and presented as a series of hyperlinks on a webpage.

All of the above are distinct from 'content producers', that is those individuals or organisations who are responsible for producing information in the first place and posting it online.

While these categories can be helpful in distinguishing the various parts of the internet,[9] it is vital to bear in mind that several of these entities offer a variety of products and services and may therefore have a number of different roles. For example, Google is probably best known as a search engine, but it also provides the Google + social media platform and the blogging platform, Blogger.

Conversely, it is also important to remember that some of these intermediaries perform the same function. For example, social media platforms, blogs and video services (e.g. YouTube) are generally considered to be 'hosts'. Although search engines are generally seen as 'technical providers', the courts have sometimes considered them to be more similar to 'hosts'. As we will see below, these distinctions are fundamental to the liability regime to which these entities may be subject.

Types of intermediary liability

There are three distinct models of liability for intermediaries:

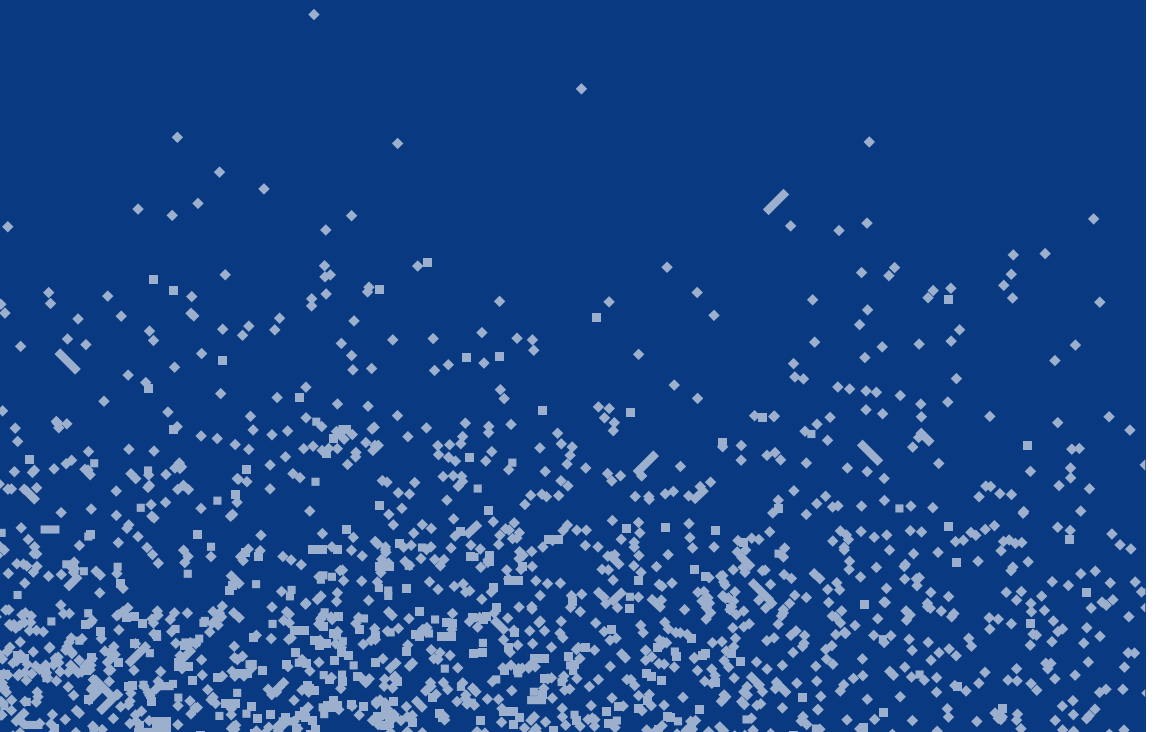
- The strict liability model under which internet intermediaries are liable for third-party content. This model is the one used, for example, in Thailand[10] and China.[11] Intermediaries are effectively required to monitor content in order to comply with the law; if they fail to do so, they face a variety of sanctions, including the withdrawal of their business licence and/or criminal penalties.
- The safe harbour model grants intermediaries immunity, provided they comply with certain requirements. This model is at the heart of the so called 'notice and take down' procedures (see below) and can be sub-divided into two approaches:
  - The vertical approach: The liability regime only applies to certain types of content. The most well-known example of this approach is the US Digital Copyright Millennium Act 1998 (DMCA) which lays down a specific 'notice and take down' procedure to deal with complaints about copyright infringement.[12] Other countries have adopted similar procedures.[13]
  - The horizontal approach: Different levels of immunity are granted depending on the type of activity at issue. This model is based on the E-Commerce Directive (ECD) in the European Union[14] where almost complete immunity is provided to intermediaries who merely provide technical access to the internet such as telecommunications service providers or ISPs (the 'mere conduit principle') and to caches.[15] By contrast, hosts may lose their immunity if they fail to act "expeditiously" to remove or disable access to "illegal" information when they obtain actual knowledge of such content.[16] This provision effectively provides the basis for what is known as a 'notice and take down' procedure without actually fleshing it out.

In exchange for conditional immunity, governments have encouraged intermediaries to explore common, usually 'technical', solutions with various interest groups as a way of dealing with complaints relating to, for example, copyright infringement or the protection of children. This is usually done in the form of "memoranda of understanding" or "best practice codes," while "technical solutions" usually involve the use of filtering software to detect and block allegedly unlawful content.

This approach, in which the government acts as a broker, is particularly prevalent in Western countries such as France, the United Kingdom and the USA.[17] Although these procedures provide an expedient and cheap mechanism for addressing alleged wrongdoing online, ARTICLE 19 notes that, in reality, their use has a very high cost for the right to freedom of expression.

- The broad immunity model grants internet intermediaries broad or conditional immunity from liability for third-party content and exempts them from any general requirement to monitor content. With this model, intermediaries are treated as 'messengers,' who are not responsible for the content they carry, rather than as 'publishers', who are responsible for the content that they disseminate although it is produced by others. It can be found, for example, in the USA,[18] Singapore[19] or the EU.[20]

Applicable international standards



The rights to freedom of expression and freedom of information are fundamental and necessary conditions if the principles of transparency and accountability are to be achieved. These principles are, in turn, essential for the promotion and protection of all human rights in a democratic society. This section identifies international and regional standards for the protection of freedom of expression online and the liability of internet intermediaries.

Guarantees of the right to freedom of expression

Article 19 of the Universal Declaration of Human Rights (UDHR)[21] guarantees the right to freedom of expression in broad terms as a right that includes the right "to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers." The International Covenant on Civil and Political Rights (ICCPR)[22] elaborates upon and gives legal force to many of the rights articulated in the UDHR. Article 19 of the ICCPR states that:

> Everyone shall have the right to freedom of opinion.
> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

In September 2011, the UN Human Rights Committee (HR Committee), a treaty monitoring body for the ICCPR, issued General Comment No 34 in relation to Article 19, which clarifies a number of issues relating to freedom of expression on the internet.[23] Importantly, it states that:

> Article 19 of ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and internet-based modes of expression.[24]
>
> States parties to the ICCPR must consider the extent to which developments in information technology, such as internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[25] In particular, the legal framework regulating the mass media should take into account the differences between the print and broadcast media and the internet, while also noting the ways in which media converge.[26]

Similarly, the four special mandates on the right to freedom of expression have highlighted in their Joint Declaration on Freedom of Expression and the Internet of June 2011 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the internet.[27] In particular, they recommend that tailored approaches for responding to illegal online content should be developed, while pointing out that specific restrictions for material disseminated over the internet are unnecessary.[28] They also promote the use of self-regulation as an effective tool in redressing harmful speech.[29]

Limitations on the right to freedom of expression

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms. Article 19(3) of the ICCPR permits the right to be restricted in the following respects:

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order, or of public health or morals.

Restrictions on the right to freedom of expression must be strictly and narrowly tailored and may not put the right itself in jeopardy. The method of determining whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must: (i) be provided by law; (ii) pursue a legitimate aim; and (iii) conform to the strict tests of necessity and proportionality.

The same principles apply to electronic forms of communication or expression disseminated over the internet. In particular, the UN Human Rights Committee noted that:

> Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.[30]

Intermediary liability under international standards

International bodies have also commented on liability regimes for intermediaries. For example, in their 2011 Joint Declaration on Freedom of Expression and the Internet, the four special rapporteurs on freedom of expression recommended that:

> No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information;
>
> Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;

> ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown.[31]

Similarly, in 2011, the UN Special Rapporteur on freedom of expression stated that:

> Censorship measures should never be delegated to a private entity, and […] no one should be held liable for content on the internet of which they are not the author. Indeed, no State should use or force intermediaries to undertake censorship on its behalf.[32]

He further recommended that, in order to avoid infringing internet users' right to freedom of expression and right to privacy, intermediaries should only implement restrictions to these rights after judicial intervention; that intermediaries should be transparent about measures taken with the user involved and, where applicable, with the wider public; that they should provide, if possible, forewarning to users before implementing restrictive measures; and they should strictly minimise the impact of any restrictions to the specific content involved.[33] Finally, the Special Rapporteur has emphasised the need for effective remedies for affected users, including the possibility of appeal using procedures to be provided by the intermediary and by a competent judicial authority.[34]

International bodies have also criticised 'notice and take down' procedures as they lack a clear legal basis. For example, the 2011 OSCE report on Freedom of Expression on the internet highlighted that:

> Liability provisions for service providers are not always clear and complex notice and takedown provisions exist for content removal from the Internet within a number of participating States. Approximately 30 participating States have laws based on the EU E-Commerce Directive. However, the EU Directive provisions rather than aligning state level policies, created differences in interpretation during the national implementation process. These differences emerged once the provisions were applied by the national courts.[35]

These procedures have also been criticised for being unfair. Rather than obtaining a court order requiring the host to remove unlawful material (which, in principle at least, would involve an independent judicial determination that the material is indeed unlawful), hosts are required to act merely on the say-so of a private party or public body. This is problematic because hosts tend to err on the side of caution and therefore take down material which may be perfectly legitimate and lawful. For example, in his report, the UN Special Rapporteur on freedom of expression noted:

> [W]hile a notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown. Moreover, given that

intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by overcensoring potentially illegal content. Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences.36

Intermediary liability: the debate

Governments and others arguing in favour of the liability of intermediaries usually present two main justifications for such measures:

– As a matter of practicality, it is argued that intermediaries are best placed to block, filter or remove the material at issue since they have the technical and financial means to do so.

– As a matter of fairness, it is argued that intermediaries should offer solutions to the challenges their activities present for law enforcement and other groups (such as copyright holders or parents).[37] In other words, since internet intermediaries benefit from disseminating third-party content online (through advertising or the payment of subscription fees), they should bear responsibility for preventing access to illegal or harmful material.

ARTICLE 19 believes that these views are misguided and wrong for several reasons:

– Firstly, the fact that intermediaries have the technical means to prevent access to content does not mean that they are the best placed to evaluate whether the content in question is "illegal" or not. Such determination should be, first and foremost, a matter for an independent – preferably judicial – body, and not a private intermediary. This is not simply a matter of intermediaries not having the relevant legal expertise to make such judgments, but a more fundamental matter of legal principle: i.e. that measures affecting fundamental rights should be applied by an independent court rather than by private bodies. Moreover, many intermediaries are likely to have their own conflicts of interest in such matters: the willingness of Google, for example, to yield to takedown requests from copyright holders may well be affected by its own commercial decision to develop a streaming service or a product similar to iTunes.

– Secondly, experience shows that procedures under limited liability regimes ('notice and take down' procedures) frequently fall well below the standards of basic fairness that could be expected of even the most summary procedure. Hosts are effectively given an incentive to remove content promptly on the basis of allegations made by a private party or public body without a judicial determination of whether the content at issue is unlawful. Moreover, the person who made the statement at issue is usually not given an opportunity to consider the complaint.[38] Since intermediaries tend to err on the side of caution and take down material which may be perfectly legitimate and lawful, such procedures have an overall chilling effect on freedom of expression.[39]

– Thirdly, the suggestion that intermediaries should bear responsibility for the content they disseminate ignores the basic reality that, with few exceptions,[40] intermediaries are simply providing the infrastructure for the sharing of content and have nothing to do with the content itself.

– Fourthly, requiring or allowing internet intermediaries to monitor and censor content produced by third parties not only has a profound chilling effect on the freedom of expression of internet users, but also makes them complicit in a substantial invasion of their customers' personal privacy.

ARTICLE 19's recommendations

Hosts should not be liable for third-party content: preferred model

ARTICLE 19 recommends that in order to comply with international standards on freedom of expression:

- Hosts should in principle be immune from liability for third-party content in circumstances where they have not been involved in modifying that content.
- State should not delegate censorship measures to intermediaries. Hosts should only be required to remove content following an order issued by an independent and impartial court or other adjudicatory body that has determined that the material at issue is unlawful.[41] Moreover, from the perspective of hosts, orders issued by independent and impartial bodies provide a much greater degree of legal certainty.

Notice-to-notice procedures: alternative model

ARTICLE 19 recognises that the preferred model described above might not always be possible as it might be too burdensome and costly for the courts to examine all applications for content removal given the high volume of such requests currently received by hosts.

We therefore recommend that notice-to-notice procedures should be developed as an alternative to notice and take down procedures. These would allow aggrieved parties to send a notice of complaint to the host.

In order to comply with international standards and best practice,[42] notice-to-notice systems should meet the following conditions:

- The notice sent by an aggrieved party should include minimum requirements, including:
  - the name of the complainant;
  - the statement concerned with an explanation as to why it should be considered unlawful, including the provision of a legal basis for the claim;
  - the location of the material; and
- an indication of the time and date when the alleged wrongdoing was committed. If the notice complies with these requirements, and upon payment of a fee, the host will then be required to forward the notice electronically as soon as is practicable (e.g. within 72 hours) to the person identified as the wrongdoer. They could be identified either directly by the complainant or via their IP address. The claimant will then be informed that the notice had been forwarded or, if not, why this was not possible.

- The alleged wrongdoer will then have a choice of either removing the content and informing the complainant (directly or via the host) or of filing a counter-notice within a sufficient time period (e.g. 14 days of receipt of the notice). The host will then forward the counter-notice within a set time (e.g. 72 hours) to the complainant, who will have another period of time (e.g. 14 days upon receipt of the counter-notice) to decide whether or not to take the matter to a court or other independent body with adjudicatory powers to determine the matter. Depending on the content at issue and the complexity of the complaint, consideration will be given to fast-track and low-cost procedures.
- If the alleged wrongdoer wishes to remain anonymous and refuses to give their contact details when filing the counter-notice, the complainant would have to seek a disclosure order from the court in order to bring the matter before the courts. This would at least stem the tide of abusive claims by adding the additional hurdle of convincing a court that disclosure was necessary. In this scenario, the only remedy available to claimants against online service providers would be statutory damages for failing to comply with their 'notice-to-notice' obligations.
- If the alleged wrongdoer fails to respond or file a counter-notice within the required time limit, the host will lose its immunity from liability. In other words, the host will have a choice. It can either take the material down or decide not to remove it, in which case it may be held liable for the content at issue if the complainant wishes to take the matter to a court or other independent adjudicatory body.

ARTICLE 19 believes that this system would work well when dealing with civil claims relating to copyright, defamation, privacy, adult content and bullying (as opposed to harassment or threats of violence). In our view, such a system would at the very least give content providers the opportunity to respond to allegations of unlawfulness before any action was taken; it would contribute to reducing the number of abusive requests by requiring a minimum of information about the allegations; and it would provide an intermediate system for resolving disputes before matters were taken to court.

Content removal in cases of alleged serious criminality: model for specific cases

ARTICLE 19 recognises that notice-to-notice systems may not be appropriate for all types of content, for example, child sexual abuse images or child "pornography" or incitement to discrimination, hostility and violence[43], all of which are prohibited under international law.

ARTICLE 19 notes three ways in which a complaint about such content should be able to be made:

– First, anyone should be able to notify law enforcement of suspected criminal activity, including online criminal activity. If law enforcement authorities believe that the content at issue should be removed and the matter is not urgent, they should seek a court order, if necessary on an ex parte basis. If, however, the situation is urgent, e.g. someone's life is at risk, law enforcement should be given statutory powers to order the immediate removal or blocking of access to the content at issue.

– However, any such order should be confirmed by a court within a specified period of time, e.g. 48 hours. The use of informal mechanisms, e.g. phone calls or emails requesting the host to remove content, should not be permitted.

– Secondly, individual internet users may wish to notify the host or social media platform about suspected criminal content. In such cases, the host or platform should in turn notify law enforcement agencies if they reason to believe that the complaint is well-founded and merits further investigation. The host or platform may also decide to remove the content at issue as an interim measure in line with their terms of service.

– Thirdly, many countries have private bodies which work with law enforcement agencies and operate hotlines that individual internet users can call if they suspect criminal content has been posted online (see e.g. the Internet Watch Foundation in the UK or SaferNet in Brazil). In such cases, the hotline generally reports the content at issue to both the host and law enforcement agencies. They can then deal with it following the same process (outlined above) that they use to deal with complaints from individual internet users. The same model can be applied to other bodies, whether public or private, which receive complaints from the public concerning potentially criminal content online.

Whichever option is pursued, it is important that the authorities are notified of any allegation of serious criminal conduct so that it may be properly investigated and dealt with according to the established procedure of the criminal justice system.

It is important to bear in mind that, in many countries, criminal law often includes a large number of minor or administrative offences and it is unlikely to be in the public interest for the police to be required to investigate every allegation of potentially criminal activity online.[44] For the same reason, prosecutors should consider whether it is necessary to prosecute cases if the matter can be more effectively addressed by the removal of the content (e.g. taking down a racist remark on Twitter).[45] It is therefore worth bearing in mind that, in the majority of cases involving allegations of minor infractions of the law, it will be more proportionate to remove the content in question rather than pursue a criminal prosecution.

End notes

1 The Organisation for Economic and Cooperation and Development (OECD) defines internet intermediaries as bodies which "give access to, host, transmit and index content, products and services, originated by third parties on the internet or provide internet-based services to third parties." See Organization for Economic Cooperation and Development, The Economic and Social Role of internet Intermediaries, April 2010, p. 9.

2 See, for example, US Telecom, internet Regulation, available at: http://www.ustelecom.org/issues/using-broadband/internet-regulation.

3 For example, Freedom House notes that, of the 47 countries it recently examined, 20 had experienced negative developments since 2011. Even in those countries with notable improvements, the general trend was towards more restrictions on internet freedom See Freedom House, Freedom on the Net 2012, page 1, available at http://www.freedomhouse.org/sites/default/files/resources/FOTN%202012%200verview%20Essay.pdf

4 This is, for example, a case of Russia; New York Times, Russians selectively blocking internet, 31 March 2013, available at: http://www.nytimes.com/2013/04/01/technology/russia-begins-selectively-blocking-internet-content.html?_r=0

5 Joe McNamee, internet intermediaries: the new cyber police?, 2011, available at http://www.giswatch.org/en/freedom-association/internet-intermediaries-new-cyberpolice.

6 See, ARTICLE 19, Wikileaks and internet companies, available at http://www.article19.org/resources.php/resource/1680/en/wikileaks-and-internet-companies. See also, PayPal Admits State Department Pressure Caused It To Block WikiLeaks, August 2010, available at http://www.huffingtonpost.com/2010/12/08/paypal-admits-us-state-de_n_793708.html.

7 See, for example, EFF, Free Speech Coalition Calls on PayPal to Back Off Misguided Book Censorship Policy, March 2012, available at https://www.eff.org/deeplinks/2012/03/free-speech-coalition-calls-paypal-back-misguided-book-censorship-policy; or Consumerist, PayPal Rains On Regretsy's Secret Santa Campaign Over Use Of Wrong Button, December 2011, available at http://consumerist.com/2011/12/05/paypal-rains-on-regretsys-secret-santa-campaign-over-use-of-wrong-button/

8 Later position papers will address issues such as website blocking and filtering and compliance with the Terms and Conditions of social media platforms with international standards on freedom of expression.

9 For an alternative categorisation of internet intermediaries, see for example Centre for Democracy and Technology (CDT), Shielding the Messenger: Protecting Platforms for Expression and Innovation, December 2012, available at: https://www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf.

10 Under the Thailand's Computer Crimes Act 2007 (CCA 2007), criminal sanctions can be imposed, inter alia, for publication of information on public computers in circumstances where the disseminated information is false and is likely to cause damage to a third party or the country's national security. See ARTICLE 19, UPR: Thailand, 2011, available at: http://www.article19.org/data/files/medialibrary/1739/11-03-14-UPR-thailand.pdf. Chiranuch Premchaiporn, the editor of an online news site, was famously tried and convicted under the provisions of the CCA 2007 for failing expeditiously to remove an anonymous comment, which was deemed insulting to the King.

11 The Chinese government imposes liability for unlawful content on all intermediaries. If they fail to sufficiently monitor the user of its services, take down content or report violations, they face fines, criminal liability, and revocation of its business or media license. See, for example, CTD, Shielding the Messengers: Protecting Platforms of Expression and Innovation, December 2012.

12 Digital Millennium Copyright Act, 105th Congress (1997-1998), H.R.2281.ENR.

13 See Daniel Seng, Comparative Analysis of the National Approaches to the Liability of Intermediaries, WIPO, 2011; or Ignacio Garrote Fernandez Diez, Comparative Analysis of the National Approaches to the Liability of Intermediaries for Infringement of Copyright and Related Rights, WIPO.

14 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market or 'E-commerce directive'.

15 See Article 12 and Article 13 of the ECD respectively.

16 Article 14 of the ECD.

17 In France, this is model proposed by the Lescure report of May 2013 to deal with infringing websites. In the UK, government regularly threatens mandatory network filtering to deal with several types of content, especially online child protection: see BBC, Online pornography to be blocked by default, PM to announce, 22 July 2013, available at: http://www.bbc.co.uk/news/uk-23401076. In the USA, Hollywood studios announced in 2012 a 'Six –Strikes' memorandum of understanding with a number of telecommunication companies to deal with 'online piracy'.

[18] See, Section 230 of the Communications Decency Act (CDA) 1996 which provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." However, this immunity does not apply to federal crimes, copyright infringement claims and electronic communications privacy law.

[19] See the Electronic Transaction Act 2010 of Singapore.

[20] See, for example, the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, the 'E-commerce directive' in the EU.

[21] UN General Assembly Resolution 217A(III), adopted 10 December 1948

[22] GA Res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc. A/6316 (1966); 999 UNTS 171; 6 ILM 368 (1967).

[23] General Comment No. 34, CCPR/C/GC/34, adopted on 12 September 2011.

[24] General Comment No.34, op.cit., para. 12.

[25] Ibid., para. 17.

[26] Ibid., para. 39.

[27] The 2011 Joint Declaration on Freedom of Expression and the Internet, June 2011, available at http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf.

[28] Ibid.

[29] Ibid. See also UN Special Rapporteur on Freedom of Expression, A/66/290, 10 August 2011, para. 16.

[30] General Comment No. 34, op.cit., para 43.

[31] The 2011 Joint Declaration, op. cit.

[32] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27, para. 43.

[33] Ibid. para 47.

[34] Ibid.

[35] OSCE report, Freedom of Expression and the Internet, July 2011, p. 30.

[36] See the 2011 report of the UN Special Rapporteur on Freedom of Expression, op.cit., para. 42.

[37] See, for example, OECD, The Role of Internet Intermediaries in advancing Public Policy Objectives, Workshop Summary, 2010, available here: http://www.oecd.org/sti/ieconomy/45997042.pdf

[38] This is at least how the ECD has been applied in practice in several Member States, see ARTICLE 19, Response to EU consultation on the E-Commerce Directive, November 2010, available at: http://www.article19.org/data/files/pdfs/submissions/response-to-eu-consultation.pdf

[39] See the 2011 report of the UN Special Rapporteur on the right to freedom of expression, op.cit., para. 42.

[40] The exceptions include social media platforms, such as Facebook and similar sites, whose business model depends on promoting a 'safe and clean' social space. However, even these platforms done not interfere with a user's content when it comes to private messages exchange between users.

[41] Cf. the regime under Section 230 of the CDA in the USA, op.cit.; or the system in Chile for copyright infringement; see CDT, Chile's notice-and-takedown system for copyright protection: an alternative approach, August 2012: https://www.cdt.org/files/pdfs/Chile-notice-takedown.pdf

[42] Cf. the system in Canada under the Bill C-11, the Copyright Modernization Act; available at: http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5686009&File=78#18

[43] Cf. the 2011 report of the UN Special Rapporteur on the right to freedom of expression, op.cit.

[44] In the UK, see for example, the Twitter Joke Trial case: http://www.article19.org/resources.php/resource/3352/en/england-and-wales:-criminalising-twitter-airport-joke-violates-free-expression

[45] For more details, see ARTICLE 19's response to the DPP's consultation on social media prosecutions, March 2013, available at: http://www.article19.org/data/files/medialibrary/3657/Social-media-prosecution_ARTICLE-19-response.pdf