ARTICLE 19

Freedom of Expression Unfiltered: How blocking and filtering affect free speech

December 2016

Policy Brief

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: 978-1-910793-15-2~~

The Principles were developed as a part of the Civic Space Initiative financed by the Swedish International Development Cooperation, Sida. Sida does not necessarily share the opinions here within expressed. ARTICLE 19 bears the sole responsibility for the content of the document.

Executive summary

In this policy brief, ARTICLE 19 outlines its position on the compatibility of blocking and/or filtering of online content with international standards on human rights, in particular the right to freedom of expression.

The policy brief is motivated by concerns about developments - in authoritarian and democratic countries alike - whereby freedom of expression online is restricted through the blocking/filtering of content that governments deem "illegal". It deals with blocking/filtering of content on websites at network level (hence, in this document, the term "blocking/filtering" only refers to these types of measures). ARTICLE 19 is concerned about these measures for several reasons:

- First, technical restrictions on access to content are prima facie an interference with the fundamental right of every person to exchange information and ideas;

- Second, blocking measures in particular are notoriously ineffective, carrying the risks of both over-blocking and under-blocking and as such are a violation of the right to freedom of expression;

- Third, blocking/filtering decisions usually lack transparency and are rarely ordered by a court. Very often, they are adopted by either administrative authorities or through so-called 'voluntary' cooperation with service providers. As a result, many governments are now in breach of their obligations under international human rights law through their use of blocking/filtering technologies. Even more disturbingly, vast swathes of information are disappearing from the Internet without users even noticing.

For these reasons, ARTICLE 19 rejects the use of blocking/filtering as a matter of principle. Nonetheless, we explain that blocking can only ever be compatible with international standards on freedom of expression where it has been provided by law and a court has determined that a blocking measure is necessary in order to protect the rights of others, or where filtering has been voluntarily adopted by the individual user.

This policy brief is divided into four parts. First, we provide basic definitions and terminology concerning blocking/filtering. This is followed by an outline of relevant international standards on freedom of expression. We then address the fundamental issues underlying the use of filters and blocking measures. Finally, we provide comprehensive recommendations for legislators, policy and decisions makers in this area.

Summary of recommendations

1. Blanket filtering must be prohibited by law;
2. Filtering should be user-controlled and transparent;
3. Any requirement to block content must be provided by law;
4. Blocking should only be ordered by an independent and impartial court or adjudicatory body;
5. Blocking orders must be strictly proportionate to the aim pursued.

Table of contents

Introduction

The Internet was designed to enable the free flow of information; however, technical measures restricting access to content are now worryingly commonplace in authoritarian and democratic countries alike. Whereas the Great Firewall of China used to be the most extreme example of how repressive governments seek to restrict freedom of expression online, European countries now increasingly rely on blocking measures to restrict access to copyright infringing or "extremist" websites.[1]

Although a growing number of countries are turning to the removal of content rather than merely blocking access to it,[2] ARTICLE 19 remains deeply concerned by content blocking/filtering.

- Firstly, these measures are prima facie an interference with the fundamental right of every person to seek and exchange information and ideas.

- Secondly, they are notoriously ineffective, as they involve risks of both over-blocking and under-blocking content and as such amount to a violation of the right to freedom of expression.

- Thirdly, blocking/filtering decisions usually lack transparency and are rarely ordered by a court. More often than not, they are adopted by either administrative authorities or through so-called 'voluntary' cooperation with service providers.

As a result, many governments are now in breach of their obligations under international human rights law as a result of their use of blocking/filtering technologies.[3] Even more disturbingly, vast swathes of information are disappearing from the Internet without users even noticing. Blocking/filtering also contribute to the fragmentation of the Internet by reinstating borders, contrary to the medium's architecture and design.

In response to these developments, this ARTICLE 19 policy brief addresses the issues raised by the blocking/filtering of content on websites at network level. In particular, we review whether blocking and filtering can ever be compatible with international human rights standards, and offer a series of recommendations which the courts or independent adjudicatory bodies should take into consideration when reviewing blocking requests.

While ARTICLE 19 rejects the use of filters and blocking measures as a matter of principle, we include recommendations as to the compatibility of such measures with international human rights standards.

Blocking/filtering: the basics

Definitions and terminology

"Filtering" and "blocking" are terms which are often used interchangeably to refer to activities aimed at preventing Internet users from accessing certain content. Due to the technical complexity of the Internet, blocking/filtering can easily be confused with other measures which are employed to deal with undesirable or unlawful content.

- **Definition of blocking and filtering:** the difference between "filtering" and "blocking" is a matter of scale and perspective.[4]
  - Filtering is commonly associated with the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords, or on the basis of their perceived connection to content deemed inappropriate or unlawful;[5]
  - Blocking, by contrast, usually refers to preventing access to specific websites, domains, IP addresses, protocols or services included on a blacklist.[6]

In this policy, ARTICLE 19 focuses solely on the blocking/filtering of content on websites at network level, which can be done by Internet service providers (ISPs), Internet exchange points (IXPs), registries and other parts of the Internet infrastructure. We do not address other types of blocking/filtering, for instance in the context of spam, self-censorship or content removal on third-party platforms.

- **Blocking/filtering are distinct from content removal or 'takedown':** blocking/filtering restrict access to content which continues to exist on the network, whereas the effect of content removal or 'takedown' is that the content itself no longer exists because it is removed from the server where it is stored.[7]

- **Monitoring is a pre-requisite for blocking and/or filtering:** "monitoring" is a term that can describe anything from the capability of systems administrators and ISPs to oversee the flow of traffic on their networks, to the full-blown interception of the content of communications by law enforcement agencies or intelligence services. Monitoring can be either passive or active.

  - Passive monitoring involves searching for specific protocols, patterns or keywords;

  - Active monitoring, by contrast, involves the close inspection of data traffic using techniques such as Deep Packet Inspection.[8] Whilst active monitoring is commonly – but not exclusively - used for surveillance purposes, passive monitoring is usually associated with blocking/filtering.

There is an obvious distinction, however, between monitoring the data, which flows across a network, and filtering/blocking it. At the same time, it is important to bear in mind that monitoring data traffic is a precondition for filtering and/or blocking. Most recently, the increasing use of protocols which encrypt data and metadata, such as TLS (colloquially know as HTTPS), have made the granular monitoring of content – and therefore precise blocking - more difficult.[9]

- **Network filtering is distinct from filtering by services:**

  - Network level filtering impacts users' access to certain websites, applications and protocols;

  - Filtering by services is used by providers of services - such as Google, Twitter or YouTube - as part of their internal policing of their email, search and content sharing services and platforms.[10] While the latter is problematic in its own right, it will be examined in a different ARTICLE 19 policy.

Types of blocking/filtering

There are several types of blocking measures that can be used to restrict access to content on the Internet with varying degrees of precision.[11] The most common methods used, either alone or combined, include:[12]

- **Uniform Resource Locator (URL) blocking,** which allows the blocking of specific web pages and page elements such as images;

- **Internet Protocol (IP) address blocking,** which prevents users from connecting to a host (which may host many separate websites);

- **Domain Name System (DNS) tampering,** which restricts access to entire domain names;

- **Protocol blocking,** which prevents access to certain types of networks such as peer-to-peer networks or Virtual Private Networks (VPN).

Filtering is usually implemented in the following ways:[13]

- **Blacklists** – the software compiles a list of URLs or content to be filtered;

- **Whitelists** – the software compiles a list of 'authorised' URLs, i.e. that are not subject to blocking or filtering;

- **Keyword blocking** – the software blocks content according to a list of keywords, such that websites containing one or more of these key words are blocked;

- **Deep Packet Inspection (DPI)** – this technique scans the content of each data packet that passes through a network. This implementation method is significantly different from those outlined above as it involves a deeper level of analysis of data traffic. DPI is commonly used for network management purposes, e.g. to filter out viruses and spam. If used for surveillance or filtering purposes, however, it significantly interferes with the right to privacy and freedom of expression.

The above filtering mechanisms are not mutually exclusive. For instance, blacklists and whitelists can be operated alongside one another and combined with keyword blocking and content rating.

Application of filters

Blocking/filtering can be implemented at several different levels, including - but not limited to - the following:

- **National level** – when governments require all Internet Service Providers to apply filters nationwide;
- **ISP level** – affecting all of the customers of a specific ISP;
- **Company network filtering** – filters are often applied to computers in workplaces or school/university campuses, and implemented on a contractual basis between users and the company;
- **End-user level** – a user decides to apply filters to his or her Internet connection or device, e.g. parental control software on a tablet.

Blocking/filtering orders

Under international human rights standards, the blocking/filtering of content should be ordered by a court or other independent adjudicatory bodies.[14] However, in some countries, it is ordered by government departments or other public agencies.[15] Orders might also take place through informal channels with the relevant government agency contacting ISPs directly by phone and asking them to block specific content.[16]

Filtering can occur as a result of legislation that imposes direct obligations on ISPs to filter certain types of content.[17] Failure to comply with these obligations is usually punished by sanctions ranging from withdrawal of a license to provide telecommunications services to imprisonment.[18]

By contrast, filtering may also be applied voluntarily, either because the end-user decides to enable filters on his or her own device or Internet connection, or because an intermediary (typically an ISP or hosts) wants to prevent its customers from viewing certain types of content.

Applicable international human rights standards

The right to freedom of expression under international law

The right to freedom of expression is guaranteed by a number of international instruments, including Article 19 of the Universal Declaration of Human Rights (UDHR)[19] and Article 19 of the International Covenant on Civil and Political Rights (ICCPR).[20] Importantly, Article 19 (1) of the ICCPR provides that the right to freedom of expression includes the individual's freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media of his choice.

In September 2011, the UN Human Rights Committee (HR Committee), the UN treaty-monitoring body, expressly recognised that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[21] The HR Committee also recommended that the legal framework regulating the mass media should take into account the differences between the print and broadcast media and the Internet, as well as the ways in which media converge.[22]

Similarly, the four special mandates for the protection of freedom of expression highlighted in their 2011 Joint Declaration on Freedom of Expression on the Internet that regulatory approaches in the telecommunications and broadcasting sectors could not simply be transferred to the Internet.[23] In particular, they recommended the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet were unnecessary. They also promoted the use of self-regulation as an effective tool in countering harmful speech.[24]

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 subject to three specific conditions, which are often articulated as the three-part test. In particular, restrictions must:

- Be provided by law;
- Pursue one or more of the legitimate aims exhaustively listed under Article 19 (3), namely respect for the rights or reputations of others, the protection of national security or public order, public health or morals; and
- Be strictly necessary and proportionate in a democratic society. Importantly, restrictions on the right to freedom of expression must be interpreted and applied strictly and narrowly.

The same principles apply to electronic forms of communication or expression disseminated over the Internet. In particular, the HR Committee has said in its General Comment No 34 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.[25]

International standards on blocking/filtering

International human rights bodies have expressed their deep concern about blocking/filtering measures.[26] In particular, the four special mandates on freedom of expression in their 2011 Joint Declaration on Freedom of Expression on the Internet held that:[27]

1. Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.

2. Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression.

3. Products designed to facilitate end-user filtering should be required to be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering.

At the same time, the UN Special Rapporteur has recognised that website blocking may be justified in limited circumstances in order to deal with categories of content which are prohibited under international law, namely: child sex abuse images (child pornography), incitement to commit genocide, advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, and incitement to terrorism.[28] In the case of child pornography, he opined that this was one of the clear exceptions where website blocking may be justified.

Nonetheless, he made it absolutely clear that blocking measures must always comply with the three-part test under Article 19(3) ICCPR.[29] In this respect, he laid down some minimum criteria that must be met in order for website blocking and filtering to be justified under international law, namely:[30]

- Blocking/filtering provisions should be clearly established by law;
- Any determination on what content should be blocked must be undertaken by a competent judicial authority or body which is independent of any political, commercial, or other unwarranted influences;

– Blocking orders must be strictly limited in scope in line with the requirements of necessity and proportionality under Article 19 (3);

– Lists of blocked websites together with full details regarding the necessity and justification for blocking each individual website should be published;

– An explanation as to why a page has been blocked should also be provided on a page that is substituted in for the affected websites;

The above standards have been echoed by regional mechanisms for the protection of human rights, including the Council of Europe,[31] the European Court of Human Rights[32] and the OAS Special Rapporteur on Freedom of Expression.[33] Importantly, they have confirmed that:

– Search engines and other intermediaries should not be required to monitor their networks proactively in order to detect possible illegal content;[34]

– It should be possible to challenge blocking and filtering orders before an independent and impartial tribunal and seek clarification and remedies.[35] In this regard, the HR Committee has clarified that there should be no generic bans on the operation of sites or systems.[36]

More generally, international human rights bodies have recommended that filtering be end-user controlled, and that at minimum, users should be informed when a filter is active and given as much control as possible over the level of filtering.[37]

Blocking/filtering: key issues

Proportionality of blocking/filtering under international human rights law

Blocking/filtering are sometimes presented as a remedy to various social ills, from sex abuse images, adult pornography, intellectual property infringement, privacy violations, defamation, illegal gambling, and "hate speech", to terrorism or other national security threats.

Typically, these measures are aimed at:

– Preventing users from accessing certain types of content to protect them (e.g. child sex abuse images) or a third party (e.g. privacy violation); or

– Preventing users from downloading illegal material (e.g. 'pirate' websites) and potentially committing an offence (e.g. accessing child sex abuse images). In this sense, blocking/filtering can be framed as measures to combat and reduce criminality.

Before such measures are adopted or implemented, however, the key question that must be answered is whether blocking/filtering are necessary and proportionate to tackle the problems they are purported to address. The response very much depends on the technology being used to block/ filter content and its impact on the rights to freedom of expression and privacy, as some technologies are more intrusive than others. If the answer is in the negative, then website filtering and blocking should not be implemented at all.

In ARTICLE 19's view, blocking/filtering are disproportionate under international human rights law for the following reasons:[38]

– **Over-blocking or 'false positives'**: no system can ensure that legitimate content is not wrongfully restricted. In particular, legitimate sites may be blocked because they use the same IP address as "unlawful" sites;[39]

– **Under-blocking' or 'false negatives'**: conversely, sites containing illegal or targeted content might not be caught by the blocking/filtering system. This is particularly problematic in the case of online child protection as parents derive a false sense of security from the knowledge that web-blocking measures are in place;

– **Failure to address the root causes**: blocking/ filtering do not address the root causes of the particular problem at issue and are no substitute for law enforcement and the prosecution of serious crimes committed over the Internet.[40]

– **Possibility of circumvention**: blocks/filters are generally relatively easy to circumvent both by sufficiently tech-savvy end-users and "criminals" when they detect that they have been added to a blocking list;

– **Failure to consider the changing nature of websites**: website blocking, as opposed to blocking of specific webpages, ignores the fact that the content of websites is liable to change over time, often significantly;[41]

– **Violation of human rights**: granular blocking/filtering strategies are deeply intrusive of users' right to privacy and freedom of expression as they analyse the content of the material exchanged between users;

– **Interference with the Internet infrastructure**: blocking/filtering interfere with several critical elements of the Internet's infrastructure and design, and causes reduction in traffic speed and financial burdens on Internet intermediaries.[42]

In short, blocking/filtering are profoundly inimical to freedom of expression and human rights whilst not being effective at tackling the problems they are purported to address. They are therefore disproportionate and should not be implemented.

Permissibility of voluntary filtering under international human rights law

Unfortunately, governments often decide that blocking/filtering should be applied regardless of the well-documented lack of effectiveness of these measures. When that is the case, the key issue becomes how blocking and filtering are implemented and more specifically, whether these measures are provided by law or "voluntary" agreements. In a large number of countries, decisions to block/ filter content are opaque. In particular, blocking powers are rarely expressly provided by law.[43] When that is the case, the restriction is per se illegal under international law.

Moreover, because governments are prohibited from imposing blanket filtering in certain countries,[44] they have sought to encourage intermediaries to 'cooperate' with them or other stakeholders in combating content deemed unlawful or harmful. In some countries, they have put pressure on ISPs to install filters by default on the Internet connection of their customers, who can request to opt-out of the filters.[45]

In ARTICLE 19's view, this system is deeply problematic for several reasons:

– Given the impracticality of contacting ISPs to request an opt-out, many people are likely to leave the filters on;

– Neither the categories of filtered content or the way in which the categories are applied in individual cases are transparent to the end-user;

– Potentially thousands of websites are blocked because they fall within one of the categories of harmful content put in place by the ISPs;

– Legitimate websites which are being filtered are not notified that their content might be filtered;

– There is no mechanism for websites to challenge being wrongfully placed on a blacklist of sites that must be blocked.

Voluntary filtering of this kind might also violate the right to freedom of expression under international law:

- Voluntary measures are, almost by definition, not provided by law. This includes, for instance, measures adopted by ISPs of their own accord. At the same time, voluntary agreements promoted or brokered by states almost certainly amount to government measures without a legal basis;

- The absence of a legal basis means that there is no requirement to clarify the categories of content subject to filtering or offering mechanisms of redress for wrongful filtering;

- It effectively places ISPs in the position of having to decide which types of content should be filtered, which is wholly inappropriate. As profit-making enterprises, ISPs are ill suited to make neutral decisions as to the kinds of content that should or should not be blocked/filtered. In particular, they have neither the required independence, nor are they sufficiently qualified, to make decisions about the legality of material, much of which they would have little or no formal knowledge about;

- To the extent that the underlying purpose of this type of voluntary filtering is to circumvent the prohibition on mandatory filtering, it is also likely to be contrary to the rule of law; while it may be more socially acceptable than mandatory network filtering, the net effects are likely the same.

By contrast, user-controlled filtering is proportionate since it remains entirely the decision of each individual to determine the type of content to which he or she does not wish to gain access. In this sense, the decision of a private individual to purchase filtering software for his or her own use does not offend human rights standards, for it is for each individual to make decisions about which types of material they wish to be exposed to online, so long as they are aware of the attendant risks of over-blocking and other issues.

Equally, Internet filtering may be acceptable if users give their informed consent to filters being applied by their ISP as a strictly opt-in measure. At the same time, filtering by contract cannot be used to negate the prohibition on content monitoring for the reasons outlined above.

ARTICLE 19's recommendations

Recommendation 1: Blanket filtering must be prohibited by law

Internet intermediaries should never be required to monitor their networks proactively in order to detect possible illegal content. Blanket filtering should be explicitly prohibited by law.

Recommendation 2: Filtering should be user-controlled and transparent

Filtering should be user-controlled and not imposed by governments or internet intermediaries. Users who do not wish to be exposed to certain types of content should be free to decide for themselves not to get access to it without restricting others' ability to access the same content.

To the extent that ISPs may wish to apply filtering measures by virtue of a contract with users, such measures should be transparent. In particular, everyone affected should be able to understand the criteria according to which the filtering operates; for example, blacklists, whitelists, keyword blocking, content rating and others should be clearly specified.[46] Moreover, users should at the very least be given an opportunity to opt-out from the application of filters, which prevent them from accessing certain types of content.

Recommendation 3: Any requirement to block unlawful content must be provided by law

Blocking is a disproportionate interference with the right to freedom of expression as it is ineffective to achieve its stated purpose. However, to the extent that governments seek to impose blocking measures, any such measure must be provided by law. Moreover, blocking should only be permitted in respect of content which is unlawful or can otherwise be legitimately restricted under international standards on freedom of expression. Accordingly, any law providing for blocking powers should do the following:[47]

- Specify the categories of content that can be lawfully blocked, consistent with international standards on freedom of expression;
- Specify the level or levels at which blocking may be applied and the kinds of technologies that may be used; in this regard, before using specific technologies, impact assessments should be carried out to determine whether the proposed technologies have a detrimental impact on freedom of expression and the right to privacy and whether alternative, less intrusive, methods could be used to achieve the same purpose;
- Specify that blocking should only be authorised by an independent and impartial court with related procedural safeguards under the rule of law.

Recommendation 4: Blocking should only be ordered by an independent and impartial court or adjudicatory body

Insofar as blocking may already be permitted by law, this measure should only be imposed by the courts or other independent and impartial adjudicatory bodies.

Moreover, in order for blocking orders to be maximally compatible with international human rights standards, the following procedural safeguards should be put in place:

- When a public authority or third party applies for a blocking order, ISPs or other relevant internet intermediaries must be given the opportunity to be heard in order to contest the application;
- There should similarly be procedures in place allowing other interested parties, such as free expression advocates or digital rights organisations, to intervene in proceedings in which a blocking order is sought;

- Users must also be given a right to challenge, after the fact, the decision of a court or public body to block access to content.[48] Whenever certain content has been blocked by such an order, moreover, anyone attempting to access it must be able to see that it has been blocked and a summary of the reasons why it was blocked, in order that they may have the opportunity to challenge the decision.[49] In particular, blocked pages should contain the following minimum information:
  - The party requesting the block;
  - The legal basis for the decision to block; the reasons for the decision in plain/user friendly language (not legal jargon); and HTTP status code 451[50] should be served;
  - The case number, if any, together with a link to the relevant court order;
  - The period during which the order is valid;
  - contact details in case of an error;
  - Information about avenues of appeal or other redress mechanisms.

Finally, in countries where blocking decisions are already authorised by public authorities, it is vital that at a minimum, these authorities are independent of government and that their decisions are subject to prompt review by an independent and impartial court or tribunal.[51]

ARTICLE 19 notes, however, that we do not support this regulatory model as government agencies are more likely to err on the side of caution and call for measures that protect the interests they are tasked to protect, such as national security or child safety, rather than freedom of expression or privacy.

Recommendation 5: Blocking orders must be strictly proportionate to the aim pursued

Any order to block access to content should be limited in scope and strictly proportionate to the legitimate aim pursued.[52] In determining the scope of any blocking order, the courts should address themselves to the following:[53]

- Any blocking order should be as narrowly targeted as possible;
- Whether the blocking order is the least restrictive means available to deal with the alleged unlawful activity, including an assessment of any adverse impact on the right to freedom of expression;
- Whether access to other lawful material will be impeded and if so to what extent, bearing in mind that in principle, lawful content should never be blocked;
- The overall effectiveness of the measure and the risks of over-blocking;
- Whether the blocking order should be of limited duration: in this regard, ARTICLE 19 considers that blocking orders to prevent future unlawful activity are a form of prior censorship and as such are a disproportionate restriction on freedom of expression.
- Whether the list of banned sites should be made public by ISPs and/or the authorities concerned. ARTICLE 19 believes that such lists should be made public as a matter of principle. At the same time, the courts should be able to order that the list should be kept private when it is more likely than not that it would be used to circumvent the blocking order.

About ARTICLE 19

ARTICLE 19 is an international human rights organisation, founded in 1986, which defends and promotes freedom of expression and freedom of information worldwide.

It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information. An increasingly important means to express oneself and to seek, receive and impart information is through information and communication technologies such as the Internet. Hence, ARTICLE 19 has been promoting the Internet freedoms for over 10 years and is active in developments in policy and practice around freedom of expression and the Internet through our network of partners, associates and expert contacts.

ARTICLE 19 encourages organisations and individuals to give us feedback about how this policy brief is being used. Please send your feedback to legal@article19.org.

References

1. For a detailed comparative analysis of blocking and filtering practices in Europe, see Council of Europe, Comparative study on filtering, blocking and take down of illegal content on the Internet, December 2015. See in particular country reports.
2. Freedom House, Freedom on the Net, 2015.
3. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report to the Human Rights Council (May 2011 Report of the SR on FOE), A/HRC/ 17/27, 16 May 2011.
4. See IETF, Blocking and Filtering Considerations, RFC 7754, March 2016
5. For a short introduction to filtering, see Open Net Initiative
6. Ibid.
7. Servers are computers, which perform essential functions by centralising and managing requests from other computers that form part of a network. For more details about content removals, see ARTICLE 19, Internet Intermediaries: Dilemma of Liability, 2013.
8. For more detailed explanation of the DPI, see the next section.
9. See Freedom House, op. cit., p. 6.
10. See e.g. PC World, Google Explains Gmail Spam Filtering Process, 20 March 2012.
11. Each of these methods also has various implications for the integrity of the network, i.e. the very architecture of the Internet.
12. Open Net Initiative, op.cit.
13. R. S. Rosenberg, Controlling Access to the Internet: The Role of Filtering.
14. See e.g. Twentieth Century Fox Film Corporation and others v British Telecom Plc [2011] EWHC 1981 (Ch)
15. See, e.g. CLD, Russia: Comments on Internet content restrictions, July 2013.
16. See e.g. For example Azerbaijan, The Expression Online Initiative, Searching for Freedom: Online Expression in Azerbaijan, November 2012.
17. See e.g. Vietnam, Open Net Initiative, Access Denied, Country Profile: Vietnam, 7 August 2012
18. See e.g. Indonesia, ARTICLE 19, Navigating Indonesia's Information Highway, March 2013.
19. UN General Assembly Resolution 217A(III), adopted 10 December 1948.
20. The ICCPR legally binds 168 states to respect its provisions and implement its framework at the national level.
21. General Comment No. 34, CCPR/C/GC/34, adopted on 12 September 2011, para.12.
22. Ibid. para. 39.
23. See Joint Declaration on Freedom of Expression and the Internet, June 2011.
24. Ibid. See also SR on FOE, Report to the General Assembly A/66/290, 10 August 2011, para. 16.
25. General Comment No. 34, op.cit., para. 43.
26. *Ibid., para 43.*

27. The 2011 Joint Declaration, op.cit.

28. SR on FOE, 2011 Report to the General Assembly, op.cit.

29. *Ibid. para. 81*

30. *Ibid., see also the SR on FOE May 2011 report, paras. 70 and 71.*

31. Council of Europe, Recommendation of the Committee of Ministers to member states on the protection of human rights with regard to search engines, para. 12 ff.

32. European Court of Human Rights (ECtHR), Yildirim v Turkey, no. 3111/10, 18 December 2012

33. Inter-American Commission on Human Rights, Freedom of Expression and the Internet, December 2013, p.36.

34. The 2011 Joint Declaration, op.cit, para 22; Recommendation of the Committee of Ministers to member states on the protection of human rights with regard to search engines, op.cit, para. 13; EU E-Commerce Directive, article 15 and Council of Europe, Declaration on Freedom of Communication on the Internet, Principle 3; this was also confirmed by the Court of Justice of the European Union (CJEU), which held in Case C-70/10 Scarlet Extended SA v Societe belge des auteurs compositeurs et editeurs (SABAM), judgment of 24 Novembre 2011) that blanket web filtering systems installed by ISPs to prevent illegal file-sharing on peer-to-peer networks was incompatible with fundamental rights. This ruling was strongly reaffirmed in Case C-360/10 Sabam v Netlog, judgment of 16 February 2012, which raised the same question in relation to social networks.

35. The SR on FOE May 2011 report, op.cit., para, 31 and Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, 26 March 2008, Section III (vi); see also Yildirim v Turkey, op.cit., para. 64.

36. General Comment No. 34, op.cit., para 43; also Yildirim v Turkey, op.cit., para. 68

37. Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, Section I. and Recommendation on the protection of human rights with regard to search engines, op.cit, para. 16.

38. See The SR on FOE May 2011 report, op.cit., paras. 31, 32, 70, 71 and 76.

39. For instance, the UK media regulator, Ofcom, has warned that currently available blocking techniques typically carry a risk of over-blocking and are not a 100% effective: see Ofcom, Site-blocking' to reduce online copyright infringement: a review of sections 17 and 18 of the Digital Economy Act, 27 May 2011.

40. European Digital Rights Initiative, Internet Blocking: Crimes should be punished and not hidden.

41. For example Wayne Crookes v Newton, 2011 SCC 47, in which the Supreme Court of Canada concluded that there could be no liability for hyperlinking in a defamation claim.

42. Commission staff working document, "Online services, including e-commerce, in the single market," SEC(2011) 1641 final, 11 January 2012, page 51, Section 3.4.5.3 Filtering.

43. OSCE Report, Freedom of Expression on the Internet, 2011.

44. E.g. in the EU, Member States are prohibited under Article 15 of the E-Commerce Directive from imposing a general obligation on providers to monitor or store information they transmit or store.

45. For example, in the UK, throughout 2011 and 2013, the government prodded Internet Service Providers to install filters by default on the Internet connection they provide to UK residents. Users can request to opt-out of the filters, but default-filtering means that potentially thousands of websites are blocked because they fall within one of the categories of harmful content put in place by the ISPs; see e.g. BBC, Online pornography to be blocked by default, PM announces, 22 July 2013.

46. *Ibid.*

47. Council of Europe, Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, op.cit., and Recommendation CM/Rec(2012)3, op.cit., para. 16.

48. See e.g. ECtHR, Cengiz and Others v. Turkey, nos. 48226/10 and 14027/11, ECHR 2015

49. See Recommendation CM/Rec(2008)6, op.cit. Section I. and Recommendation on the protection of human rights with regard to search engines, op.cit. para 16.

50. In computer networking, HTTP 451 Unavailable For Legal Reasons is an error status code of the HTTP protocol to be displayed when the user requests a resource which cannot be served for legal reasons.

51. *Ibid., Recommendation CM/Rec(2008)6, Section III (ii) and Yildirim v Turkey, op.cit, para. 64*

52. Article 19 (3) ICCPR and Article 10 (2) of the European Convention on Human rights; Recommendation CM/Rec(2008)6, op.cit. Section III (i).

53. Yildirim v Turkey, op.cit, para. 66.

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