H/Inf (2008) 9

Human rights guidelines for Internet service providers

Developed by the Council of Europe in co-operation with the European Internet Services Providers Association (EuroISPA)

H/Inf (2008) 9

Human rights guidelines for Internet service providers

Developed by the Council of Europe in co-operation with the European Internet Services Providers Association (EuroISPA)

Directorate General
of Human Rights and Legal Affairs
Council of Europe
2008

Directorate General of Human Rights and Legal Affairs
Council of Europe
F-67075 Strasbourg Cedex

1st printing, July 2008
Printed at the Council of Europe

Developed by the Council of Europe in close co-operation with the European Internet Services Providers Association (EuroISPA), these guidelines provide human rights benchmarks for internet service providers (ISPs). While underlining the important role played by ISPs in delivering key services for the Internet user, such as access, e-mail or content services, they stress the importance of users' safety and their right to privacy and freedom of expression and, in this connection, the importance for the providers to be aware of the human rights impact that their activities can have.
For more information on the activities of the Council of Europe and ISFE: www.coe.int • www.euroispa.org

Contents

Everyone has the right to freedom of expression and information. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 10 of the European Convention on Human Rights

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 of the European Convention on Human Rights

Understanding the role and position of Internet service providers in respecting and promoting human rights

1. Internet service providers (ISPs), in providing the basic infrastructure and the basic services that allow users to access and use the Internet and thereby exercise their rights to benefit from the information society, deliver services with a significant public service value to society.

2. ISPs have a unique position and possibility of promoting the exercise of and respect for human rights and fundamental freedoms. In addition, the provision of Internet services is increasingly becoming a prerequisite for a comprehensive participatory democracy. ISPs also play an important role *vis-à-vis* states which are committed to protecting and promoting these rights and freedoms as part of their international law obligations.

3. ISPs provide a variety of services to their customers, be it as access-providers or as providers of other information society services (application-providers, content-providers and/or host-providers). It is recognised in these guidelines that not all ISPs have the same roles and responsibilities *vis-à-vis* users but that these may depend on the types of services the ISP delivers and what segment of customers the ISP serves.

4. Access-providers facilitate entry to the Internet and therefore to a diversity of information, culture and languages; they are often the first point of contact and trust for users. Their role is a prerequisite for enabling and empowering users to access the benefits of the information society, in particular to seek and impart information and ideas, to create and to access knowledge and education.

5. Access-providers, in particular those serving home-users and families, can be seen as fulfilling a part public service role that promotes their customers' rights to benefit from the information society and, to this end, strengthen the exercise and enjoyment of their rights and freedoms.

6. Equally, to the extent that access-providers and particularly host-providers may enforce decisions and actions with regard to the accessibility of services (e.g. remove, block or filter content), this can impact on rights and freedoms.

7. ISPs have access to varying amounts of information (content and/or traffic data) which underlines their important role and position vis-à-vis the rights and freedoms of users. ISPs should not be put under a general obligation to actively monitor content and traffic data; however there may be specific cases defined by law and upon specific orders where an ISP may need to assist in monitoring content or data or impart information about a user to a third party. Such cases could have an impact on freedom of expression or the right to private life.

8. Overall, there is considerable potential for ISPs, particularly host and content providers, to promote the opportunities and benefits of the information society, and this should be underlined and communicated to users, to states and, most importantly, to ISPs themselves.

9. In this regard, ISPs are encouraged to take note of, discuss and make their best efforts to comply with the following guidelines (overleaf) and to consider making reference to them on their websites and in their end-user agreements.

10. ISPs, in co-operation with associations of ISPs, member states, and, where appropriate, with the assistance of the Council of Europe, are also encouraged to make key personnel in their organisations aware of these guidelines and the issues raised therein.

11. Associations of ISPs can play an important role by assuming collective responsibility with regard to raising awareness and providing information about the issues raised in these guidelines. They are encouraged to actively promote these guidelines among their members, for instance by making reference to or incorporating them in their own codes of conduct and by providing expert knowledge.

12. As regards the information that should be provided towards customers, ISPs may choose to provide this information via associations of ISPs, particularly in the case of small enterprises and in those cases where the information is not provider-specific (such as information about risks on the Internet). Associations of ISPs can furthermore contribute to a harmonisation of user information and aggregate knowledge as regards the issues raised in the guidelines. In

addition they can provide for cooperation and exchange of knowledge with existing structures in the field of Internet safety, such as the European Union Safer Internet Plus Programme.

13. The guidelines are without prejudice to and must be read in conjunction with the obligations applicable to ISPs and their activities under national, European and international law.

Scope of these guidelines

14. The following guidelines are grouped in several chapters, according to the respective roles of the ISPs. The first chapter applies to Internet access providers (providers of on-demand or dedicated Internet access services). The second chapter applies to providers of other information society services, such as is the case for providers of hosting services, content providers and application providers. The third chapter applies to all Internet service providers accordingly.

15. The guidelines do not apply to mere transit providers.

Human rights guidelines for Internet service providers

Guidelines for ISPs providing access services

• 16. Ensure that your customers have access to information about potential risks to their rights, security and privacy online, including information on what you are doing to help your customers counter those risks. Provide information about available tools and software that your customers may use to protect themselves further. If you provide this information yourself, ensure that it is provided in the most accurate, accessible and up-to-date way possible. If you do not provide this information yourself, link your customers to adequate information resources, particularly those of associations of ISPs or networks in the field of Internet safety. In particular information on the following risks could be made available:

16.1. Illegal and/or harmful content, risks for children

• Provide information or link to information about risks of encountering or contributing to the dissemination of illegal content on the Internet as well as the risks for children of being exposed to harmful content or behaviour when they are online. The latter may include content or behaviour capable of adversely affecting the physical, emotional and psychological well-being of children, such as online pornography, the portrayal and glorification of violence and self-harm, demeaning, discriminatory or racist expressions or apologia for such conduct, solicitation (grooming), bullying, stalking and other forms of harassment. Although you will not be expected to advise on what content or behaviours are illegal and/or harmful, the information you give could usefully include:

– explanations on what you are doing to counter such content and behaviour, particularly your cooperation with hotlines against illegal content (e.g. Inhope);

– guidance on how users can protect themselves against the risks of encountering illegal and/or harmful content and

– behaviour (e.g. by linking them to relevant information on Internet safety websites);

– information on available software tools designed to protect users against illegal and/or harmful content, including information about how the tools work and can be adapted by the users to meet their individual needs.

• Provide information or link to information on what your customers can do to protect their children online. Make reference to websites with child-friendly content and to available online safety resources such as the Council of Europe Internet Literacy Handbook (www.coe.int/internet-literacy), the Council of Europe online game *Through the Wild Web Woods* (www.wildwebwoods.org) or websites of Internet safety nodes (www.saferinternet.org).

16.2. Security risks

• If appropriate, explain what you are doing to protect your customers against security risks. Such risks may concern data integrity (viruses, worms, trojans, etc.), confidentiality (e.g. when making transactions online), network security or other risks (e.g. phishing).

• Raise your customers' awareness or link your customers to further information on how to counter risks to their security on the Internet.

16.3. Privacy risks

• Provide for information or link to information about potential risks of customers to their privacy when using the Internet. Such risks may concern the hidden collection, recording and processing of data (spyware, profiling). If appropriate, link to websites of your national authorities with available information of applicable laws on privacy and protection of personal data.

• Offer further information and guidance to your customers about the technical means which they may use to protect themselves against privacy risks (anti-spyware tools etc.).

• 17. When your customers need support in dealing with the risks identified above, ensure that they can either make further enquiries in the appropriate form (e.g. telephone, e-mail, writing, personal contact) or link them to appropriate information resources.

• 18. Be careful about blocking or degrading the quality of your services for the use of certain applications or software based on a given technical protocol. If you apply bandwidth caps, filter or block certain traffic, make sure that your customers are informed about such service restrictions in a clear manner beforehand.

• 19. Cutting access to individual customer accounts constitutes a restriction on your customer's rights to access the benefits from the information society and to exercise their rights to freedom of expression and information. Cutting access should only be done for law enforcement or other legitimate and strictly necessary reasons, such as a violation of contractual obligations or intentional abuse, while having regard to legal safeguards that may be applicable under national law. The customer should, where appropriate, be properly warned and informed beforehand, be given adequate reasons for the cutting of access and be instructed of the steps to be taken to re-establish the access.

Guidelines for ISPs providing other information society services (hosting, applications and content)

• 20. Make sure any filtering or blocking of services carried out is legitimate, proportional and transparent to your customers in accordance with the Council of Europe Recommendation on measures to promote the respect for freedom of expression and information with regard to Internet filters, CM/Rec (2008) 6. Inform your customers of any filtering or blocking software installed on your servers that may lead to a removal or inaccessibility of content as well as the nature of the filtering that takes place (form of filtering, general criteria used to filter, reasons for applying filters).

• 21. In respect of filtering, blocking or removal of illegal content, you should do so only after a verification of the illegality of the content, for instance by contacting the competent law enforcement authorities. Acting without first checking and verifying may be considered as an interference with legal content and with the rights and freedoms of those creating, communicating and accessing such content, in particular the right to freedom of expression and information.

• 22. Inform your customers about your general policy dealing with complaints on alleged illegal content you might be hosting. Give clear indications to the general public on how to complain, and to your customers on how to respond to such complaints.

• 23. If you provide your customers with specific application services, such as the use of chat, e-mail, blogs etc., you should take care to ensure the use of the applications is as safe as possible and that your customers are made aware of the way the applications work. When providing facilities such as chat rooms or discussion forums, make sure that clear rules for user registration and use of nicknames are established and that users are informed about the rules in a clear manner before they start using your services.

• 24. Although you will not be expected to provide advice on what content or behaviours are illegal and/or harmful, you could usefully give information to teachers and parents on risks to children when using application services provided by you (chat rooms, messageboards etc.), in particular the risks of encountering harmful content or behaviour (grooming, bullying, etc.) when using your services.

• 25. When providing applications for e-mailing to your customers make sure that any measures you provide, such as spam-recognition or spam-filtering software, are effective (recognising or filtering spam while not interfering with legitimate e-mails) and your customers are properly informed about their functionality and methodology as well as the possibility to adapt their configuration.

• 26. If you provide content services to your customers, such as web-based information or news services, consider offering users a right of reply allowing the rapid correction of incorrect information along the lines of the minimum principles contained in the Council of Europe Recommendation (2004) 16 on the right of reply in the new media environment.

Guidelines for ISPs with regard to the right to respect for private life and data protection

• 27. Establish appropriate procedures and use available technologies to protect the privacy of users and secrecy of content and traffic data, especially by ensuring data integrity, confidentiality as well as physical and logical security of the network and of the services provided over the network. The level of protection should be adapted to the type of service you provide accordingly.

• 28. Offer further information and guidance to your customers about the technical means they may use to protect themselves against security risks to data and communications (such as anti-spyware software tools, firewalls, encryption technology or digital signatures, etc.).

• 29. When acting with regard to the communications of users (for example by allowing the interception or monitoring of users' e-mails) such action should only be undertaken in case of a legal duty to do so, on specific orders or instructions

from a competent public authority made in accordance with the law. Do not actively monitor the content of communications on your network. Furthermore, the deletion and modification of the user's correspondence (e.g. by spam-filters) should depend on the explicit consent of the user before the spam-filter, etc. is activated.

• 30. Do not to reveal the identity of users, their traffic data or the content of data accessed by them to a third party, unless under a legal duty to do so or following specific orders or instructions from the competent public authority made in accordance with the law. Requests in this respect brought to you from abroad should be handled through the competent authorities in your country.

• 31. Inform your customers in which circumstances you are under a legal duty to reveal their identification, connection or traffic data by request from law enforcement agencies etc. Such information could particularly be provided by associations of ISPs to whom you might want to link. If you receive a request to disclose such data, make sure to check the authenticity of the request and that it is made by a competent authority in accordance with the law.

• 32. Do not collect, process or store data about users, unless this is necessary for explicit, specified and legitimate purposes in accordance with data protection laws. Do not store data for longer than required by law or than is necessary to achieve the purpose of processing of the data.

• 33. Do not use personal data on users for your own promotional or marketing purposes unless the user concerned, after having been informed, has given his or her consent and this consent has not been revoked. Do not make personal data publicly available! Such publication may infringe other people's privacy and may also be prohibited by law.

Extracts from existing Council of Europe standards relevant to the roles and responsibilities of ISPs

Recommendation No. R (99) 5 of the Committee of Ministers to member states for the protection of privacy on the Internet[1]

Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways which may be incorporated in or annexed to codes of conduct

III. For Internet service providers

1. Use appropriate procedures and available technologies, preferably those which have been certified, to protect the privacy of the people concerned (even if they are not users of the Internet), especially by ensuring data integrity and confidentiality as well as physical and logical security of the network and of the services provided over the network.

2. Inform users of privacy risks presented by use of the Internet before they subscribe or start using services. Such risks may concern data integrity, confidentiality, the security of the network or other risks to privacy such as the hidden collection or recording of data.

3. Inform users about technical means which they may lawfully use to reduce security risks to data and communications, such as legally available encryption and digital signatures. Offer such technical means at a cost-oriented price, not a deterrent price.

4. Before accepting subscriptions and connecting users to the Internet, inform them about the possibilities of accessing the Internet anonymously, and using its services and paying for them in an anonymous way (for example, pre-paid access cards). Complete anonymity may not be appropriate because of legal constraints. In those cases, if it is permitted by law, offer the possibility of using pseudonyms. Inform users of programmes allowing them to search and browse anonymously on the Internet. Design your system in a way that avoids or minimises the use of personal data.

5. Do not read, modify or delete messages sent to others.

6. Do not allow any interference with the contents of communications, unless this interference is provided for by law and is carried out by a public authority.

7. Collect, process and store data about users only when necessary for explicit, specified and legitimate purposes.

8. Do not communicate data unless the communication is provided for by law.

9. Do not store data for longer than is necessary to achieve the purpose of processing.

10. Do not use data for your own promotional or marketing purposes unless the person concerned, after having been informed, has not objected or, in the case of processing of traffic data or sensitive data, he or she has given his or her explicit consent.

11. You are responsible for proper use of data. On your introductory page highlight a clear statement about your privacy policy. This statement should be hyperlinked to a detailed explanation of your privacy practice. Before the user starts using services, when he or she visits your site, and whenever he or she asks, tell him or her who you are, what data you collect, process and store, in what way, for what purpose and for how long you keep them. If necessary, ask for his or her consent. At the request of the person concerned, correct inaccurate data immediately and delete them if they are excessive, out of date or no longer required and stop the processing carried out if the user objects to it. Notify the third parties to whom you have communicated the data of any modification. Avoid the hidden collection of data.

12. Information provided to the user must be accurate and kept up to date.

1. Adopted on 23 February 1999.

13. Think twice about publishing data on your site! Such publication may infringe other people's privacy and may also be prohibited by law.

14. Before you send data to another country seek advice, for example from the competent authorities in your country, on whether the transfer is permissible. You may have to ask the recipient to provide safeguards necessary to ensure protection of the data.

Declaration of the Committee of Ministers on freedom of communication on the Internet[2]

Principle 6 – Limited liability of service providers for Internet content

Member states should not impose on service providers a general obligation to monitor content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity.

Member states should ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet.

In cases where the functions of service providers are wider and they store content emanating from other parties, member states may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.

When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the information available in the first place, as well as the corresponding right of users to the information.

In all cases, the above-mentioned limitations of liability should not affect the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of the law.

Extracts from the Explanatory memorandum to the Declaration on freedom of communication on the Internet

Principle 6 – Limited liability of service providers for Internet content

Here it is established that as a general rule intermediaries in the communication chain should not be held liable for content transmitted through their services, except in certain limited circumstances. Along the lines of Articles 12-15 of the Directive on electronic commerce, the exemptions to liability take into account the different types of activities of the intermediaries, namely providing access to communication networks, transmitting data and hosting information. The degree of liability depends on the possibilities of service providers to control the content and whether they are aware of its illegal nature. The limitations on liability do not apply if intermediaries intentionally disseminate illegal content.

1st paragraph – No general obligation to monitor

This paragraph is based on Article 15 of the Directive on electronic commerce. Member states should not impose any general obligation on service providers to monitor the information on the Internet to which they give access, that they transmit or store. Nor should they be subject to a general obligation to actively seek facts or circumstances indicating illegal activity, since this might have the effect of curbing freedom of expression.

This paragraph of Principle 6 does not prevent public authorities in member states from obliging service providers in certain cases, for example during a criminal investigation, to monitor the activities of their clients.

2nd paragraph – "Mere conduit"

In the case of mere transmission of information or providing access to communication networks, intermediaries should not be held liable for illegal content. When the role of intermediaries goes beyond that, in particular when they initiate the transmission, select the receiver of the transmission or select or modify the information transmitted, their liability may be invoked.

The activity of the intermediary which is at stake here, and which should be exempt from liability, is sometimes referred to as "mere conduit" (cf. Article 12 of the Directive on electronic commerce).

3rd paragraph – "Hosting"

In the case of hosting content emanating from third parties, intermediaries should in general not be held liable (cf. Article 14 of the Directive on electronic commerce). This does not apply, however, when the third party is acting under the control of the intermediary, for example when a newspaper company has its own server to host content produced by its journalists. However, if the host becomes aware of the illegal nature of the content on its servers or, in the event of a claim for damages, of facts revealing an illegal activity, it may reasonably be held liable. The precise conditions should be laid down in national law.

2. Adopted on 28 May 2003.

4th paragraph – "Notice and take down" procedures and freedom of expression and information

As stipulated in paragraph 3 of Principle 6 of the Declaration, service providers may be held liable if they do not act expeditiously to remove or disable access to information or services when they become aware, as defined by national law, of their illegal nature. It is to be expected that member States will define in more detail what level of knowledge is required of service providers before they become liable. In this respect, so-called "notice and take down" procedures are very important. Member States should, however, exercise caution imposing liability on service providers for not reacting to such a notice. Questions about whether certain material is illegal are often complicated and best dealt with by the courts. If service providers act too quickly to remove content after a complaint is received, this might be dangerous from the point of view of freedom of expression and information. Perfectly legitimate content might thus be suppressed out of fear of legal liability.

5th paragraph – The possibility of issuing injunctions remains intact

It is highlighted here, in line with Articles 12-14 of the Directive on electronic commerce, that despite the above-mentioned limitations of liability, the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of law, remains intact.

Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society[3]

With regard to self- and co-regulatory measures which aim to uphold freedom of expression and communication, private sector actors are encouraged to address in a decisive manner the following issues:

- private censorship (hidden censorship) by Internet service providers, for example blocking or removing content, on their own initiative or upon the request of a third party;

Recommendation No. Rec (2007) 11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment[4]

Member states, the private sector and civil society are encouraged to develop common standards and strategies to promote transparency and the provision of information, guidance and assistance to the individual users of technologies and services, in particular in the following situations:

…

vii. the removal of content deemed to be illegal with regard to the rule of law considerations;

Recommendation No. Rec (2007) 16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet[5]

Member states should adopt or develop policies to preserve and, whenever possible, enhance the protection of human rights and respect for the rule of law in the information society. In this regard, particular attention should be paid to:

- the right to private life and private correspondence on the Internet and in the use of other ICTs, including the respect for the will of users not to disclose their identity, promoted by encouraging individual users and Internet service and content providers to share the responsibility for this;

Member states should promote public discussion on the responsibilities of private actors, such as Internet service providers, content providers and users, and encourage them – in the interests of the democratic process and debate and the protection of the rights of others – to take self-regulatory and other measures to optimise the quality and reliability of information on the Internet and to promote the exercise of professional responsibility, in particular with regard to the establishment, compliance with, and monitoring of the observance of codes of conduct.

3. Adopted on 13 May 2005.
4. Adopted on 26 September 2007.
5. Adopted on 7 November 2007.

Recommendation No. CM/Rec (2008) 6 on measures to promote the respect for freedom of expression and information with regard to Internet filters

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage;

Recalling that States Parties to the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, ETS No. 5) have undertaken to secure to everyone within their jurisdiction the human rights and fundamental freedoms defined in the Convention;

Reaffirming the commitment of member states to the fundamental right to freedom of expression and to receive and impart information and ideas without interference by public authorities and regardless of frontiers, as guaranteed by Article 10 of the European Convention on Human Rights;

Aware that any intervention by member states that forbids access to specific Internet content may constitute a restriction on freedom of expression and access to information in the online environment and that such a restriction would have to fulfil the conditions in Article 10, paragraph 2, of the European Convention on Human Rights and the relevant case-law of the European Court of Human Rights;

Recalling in this respect the Declaration on human rights and the rule of law in the information society, adopted by the Committee of Ministers on 13 May 2005, according to which member states should maintain and enhance legal and practical measures to prevent state and private censorship;

Recalling Recommendation Rec (2007) 11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment, according to which member states, the private sector and civil society are encouraged to develop common standards and strategies to promote transparency and the provision of information, guidance and assistance to the individual users of technologies and services concerning, *inter alia*, the blocking of access to and filtering of content and services with regard to the right to receive and impart information;

Noting that the voluntary and responsible use of Internet filters (products, systems and measures to block or filter Internet content) can promote confidence and security on the Internet for users, in particular children and young people, while also aware that the use of such filters can impact on the right to freedom of expression and information, as protected by Article 10 of the European Convention on Human Rights;

Recalling Recommendation Rec (2006) 12 of the Committee of Ministers on empowering children in the new information and communications environment, which underlines the importance of information literacy and training strategies for children to enable them to better understand and deal with content (for example violence and self-harm, pornography, discrimination and racism) and behaviours (such as grooming, bullying, harassment or stalking) carrying a risk of harm, thereby promoting a greater sense of confidence, well-being and respect for others in the new information and communications environment;

Convinced of the necessity to ensure that users are made aware of, understand and are able to effectively use, adjust and control filters according to their individual needs;

Recalling Recommendation Rec (2001) 8 of the Committee of Ministers on self-regulation concerning cybercontent (self-regulation and user protection against illegal or harmful content on new communications and information services), which encourages the neutral labelling of content to enable users to make their own value judgements over such content and the development of a wide range of search tools and filtering profiles, which provide users with the ability to select content on the basis of content descriptors;

Aware of the public service value of the Internet, understood as people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions, entertainment) and the resulting legitimate expectation that Internet services be accessible, affordable, secure, reliable and ongoing and recalling in this regard Recommendation Rec (2007) 16 of the Committee of Ministers on measures to promote the public service value of the Internet;

Recalling the Declaration of the Committee of Ministers on freedom of communication on the Internet of 28 May 2003, which stresses that public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers, but that this does not prevent the installation of filters for the protection of minors, in particular in places accessible to them, such as schools or libraries;

Reaffirming the commitment of member states to everyone's right to private life and secrecy of correspondence, as protected by Article 8 of the European Convention on Human Rights, and recalling the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its Additional Protocol regarding supervisory authorities and transborder data flows (ETS No. 181) as well as Recommendation No. R (99) 5 of the

Committee of Ministers on the protection of privacy on the Internet,

Recommends that member states adopt common standards and strategies with regard to Internet filters to promote the full exercise and enjoyment of the right to freedom of expression and information and related rights and freedoms in the European Convention on Human Rights, in particular by:

- taking measures with regard to Internet filters in line with the guidelines set out in the appendix to this recommendation;
- bringing these guidelines to the attention of all relevant private and public sector stakeholders, in particular those who design, use (install, activate, deactivate and implement) and monitor Internet filters, and to civil society, so that they may contribute to their implementation.

Appendix to Recommendation CM/Rec (2008) 6: Guidelines

Using and controlling Internet filters in order to fully exercise and enjoy the right to freedom of expression and information

Users' awareness, understanding of and ability to effectively use Internet filters are key factors which enable them to fully exercise and enjoy their human rights and fundamental freedoms, in particular the right to freedom of expression and information, and to participate actively in democratic processes. When confronted with filters, users must be informed that a filter is active and, where appropriate, be able to identify and to control the level of filtering the content they access is subject to. Moreover, they should have the possibility to challenge the blocking or filtering of content and to seek clarifications and remedies.

In co-operation with the private sector and civil society, member states should ensure that users are made aware of activated filters and, where appropriate, are able to activate and deactivate them and be assisted in varying the level of filtering in operation, in particular by:

i. developing and promoting a minimum level of information for users to enable them to identify when filtering has been activated and to understand how, and according to which criteria, the filtering operates (for example, blacklists, whitelists, keyword blocking, content rating, etc., or combinations thereof);

ii. developing minimum levels of and standards for the information provided to the user to explain why a specific type of content has been filtered;

iii. regularly reviewing and updating filters in order to improve their effectiveness, proportionality and legitimacy in relation to their intended purpose;

iv. providing clear and concise information and guidance regarding the manual overriding of an activated filter, namely whom to contact when it appears that content has been unreasonably blocked and the reasons which may allow a filter to be overridden for a specific type of content or Uniform Resource Locator (URL);

v. ensuring that content filtered by mistake or error can be accessed without undue difficulty and within a reasonable time;

vi. promoting initiatives to raise awareness of the social and ethical responsibilities of those actors who design, use and monitor filters with particular regard to the right to freedom of expression and information and to the right to private life, as well as to the active participation in public life and democratic processes;

vii. raising awareness of the potential limitations to freedom of expression and information and the right to private life resulting from the use of filters and of the need to ensure proportionality of such limitations;

viii. facilitating an exchange of experiences and best practices with regard to the design, use and monitoring of filters;

ix. encouraging the provision of training courses for network administrators, parents, educators and other people using and monitoring filters;

x. promoting and co-operating with existing initiatives to foster responsible use of filters in compliance with human rights, democracy and the rule of law;

xi. fostering filtering standards and benchmarks to help users choose and best control filters.

In this context, civil society should be encouraged to raise users' awareness of the potential benefits and dangers of filters. This should include promoting the importance and significance of free and unhindered access to the Internet so that every individual user may fully exercise and enjoy their human rights and fundamental freedoms, in particular the right to freedom of expression and information and the right to private life, as well as to effectively participate in public life and democratic processes.

Appropriate filtering for children and young people

The Internet has significantly increased the number and diversity of ideas, information and opinions which people may receive and impart in the fulfilment of their right to freedom of expression and information without interference by public authorities and regardless of frontiers. At the same time, it has increased the amount of readily available content carrying a risk of harm, particularly for children and young people. To satisfy the legitimate desire and duty of member states to protect children and young people from content carrying a risk of harm, the proportionate use of filters can constitute an appropriate means of encouraging access to and confident use of the Internet and be a complement to other strategies on how to tackle harmful content, such as the development and provision of information literacy.

In this context, member states should:

i. facilitate the development of strategies to identify content carrying a risk of harm for children and young people, taking into account the diversity of cultures, values and opinions;

ii. co-operate with the private sector and civil society to avoid over-protection of children and young people by, *inter alia*, supporting research and development for the production of "intelligent" filters that take more account of the context in which the information is provided (for example by differentiating between harmful content itself and unproblematic references to it, such as may be found on scientific websites);

iii. facilitate and promote initiatives that assist parents and educators in the selection and use of developmental-age appropriate filters for children and young people;

iv. inform children and young people about the benefits and dangers of Internet content and its filtering as part of media education strategies in formal and non-formal education.

Furthermore, the private sector should be encouraged to:

i. develop "intelligent" filters offering developmental-age appropriate filtering which can be adapted to follow the child's progress and age while, at the same time, ensuring that filtering does not occur when the content is deemed neither harmful nor unsuitable for the group which the filter has been activated to protect;

ii. co-operate with self- and co-regulatory bodies in order to develop standards for developmental-age appropriate rating systems for content carrying a risk of harm, taking into account the diversity of cultures, values and opinions;

iii. develop, in co-operation with civil society, common labels for filters to assist parents and educators in making informed choices when acquiring filters and to certify that they meet certain quality requirements;

iv. promote the interoperability of systems for the self-classification of content by providers and help to increase awareness about the potential benefits and dangers of such classification models.

Moreover, civil society should be encouraged to:

i. debate and share their experiences and knowledge when assessing and raising awareness of the development and use of filters as a protective measure for children and young people;

ii. regularly monitor and analyse the use and impact of filters for children and young people, with particular regard to their effectiveness and their contribution to the exercise and enjoyment of the rights and freedoms guaranteed by Article 10 and other provisions of the European Convention on Human Rights.

Use and application of Internet filters by the public and private sector

Notwithstanding the importance of empowering users to use and control filters as mentioned above, and noting the wider public service value of the Internet, public actors on all levels (such as administrations, libraries and educational institutions) which introduce filters or use them when delivering services to the public, should ensure full respect for all users' right to freedom of expression and information and their right to private life and secrecy of correspondence.

In this context, member states should:

i. refrain from filtering Internet content in electronic communications networks operated by public actors for reasons other than those laid down in Article 10, paragraph 2, of the European Convention on Human Rights, as interpreted by the European Court of Human Rights;

ii. guarantee that nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights;

iii. introduce, where appropriate and necessary, provisions under national law for the prevention of intentional abuse of filters to restrict citizens' access to lawful content;

iv. ensure that all filters are assessed both before and during their implementation to ensure that the effects of the filtering are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unreasonable blocking of content;

v. provide for effective and readily accessible means of recourse and remedy, including suspension of filters, in cases where users and/or authors of content claim that content has been blocked unreasonably;

vi. avoid the universal and general blocking of offensive or harmful content for users who are not part of the group which a filter has been activated to protect, and of illegal content for users who justifiably demonstrate a legitimate interest or need to access such content under exceptional circumstances, particularly for research purposes;

vii. ensure that the right to private life and secrecy of correspondence is respected when using and applying filters and that personal data logged, recorded and processed via filters are only used for legitimate and non-commercial purposes.

Furthermore, member states and the private sector are encouraged to:

i. regularly assess and review the effectiveness and proportionality regarding the introduction of filters;

ii. strengthen the information and guidance to users who are subject to filters in private networks, including information about the existence of, and reasons for, the use of a filter and the criteria upon which the filter operates;

iii. co-operate with users (customers, employees, etc.) to improve the transparency, effectiveness and proportionality of filters.

In this context, civil society should be encouraged to follow the development and deployment of filters both

by key state and private sector actors. It should, where appropriate, call upon member states and the private sector, respectively, to ensure and to facilitate all users' right to freedom of expression and information, in particular as regards their freedom to receive information without interference by public authorities and regardless of frontiers in the new information and communications environment.

Developed by the Council of Europe in close co-operation with the European Internet Services Providers Association (EuroISPA), these guidelines provide human rights benchmarks for Internet service providers (ISPs). While underlining the important role played by ISPs in delivering key services for the internet user, such as access, e-mail or content services, they stress the importance of users' safety and their right to privacy and freedom of expression and, in this connection, the importance for the providers to be aware of the human rights impact that their activities can have.

For more information on the activities
of the Council of Europe and ISFE:
www.coe.int • www.euroispa.org

Directorate General
of Human Rights and Legal Affairs
Council of Europe
F-67075 Strasbourg Cedex