Search engine freedom: on the implications of the right to freedom of expression for the legal governance of Web search engines

van Hoboken, J.V.J.

Publication date
2012

Chapter 6: ISP Freedom

6.1 Introduction

This chapter will address the way in which the right to freedom of expression applies to the legal governance of 'access' to the public networked information environment by analyzing its proper application to the legal framework for Internet access providers. Internet access providers are an essential element in the value chains of the Internet, since they provide the connection of Internet users to the rest of the network. In regulatory debates, the role on Internet access providers in the information environment is often compared to traditional conduits such as the postal and telecommunications services. From the perspective of the right to freedom of expression, the role of access providers can intuitively be considered facilitative. They provide the means to exercise one's right to freedom of expression.

However, the analysis of the implications of the right to freedom of expression for Internet access providers is complicated by the fact that the relatively clear regulatory model for traditional conduits has not yet found its way to the digital environment. In addition, regulatory debates about the legal responsibility of Internet access providers are partly shaped by the anxiety that they may facilitate too much. Information access providers are sometimes considered points of control, placing the facilitative role of access providers with regard to the communicative interests of end-users and online information providers under pressure.[336] In other words, there is a clash between the resulting regulatory and legal pressure on Internet access providers to restrict communications and access to online information on the one hand, and their continuing role in providing unrestricted access to the Internet for end-users on the other hand. This makes an analysis of the implications of the right to freedom of expression for the legal governance of Internet access providers complex but all the more interesting. Since the debate about the responsibility of search engine providers has been subject of a similar conflict of interests and arguments, this analysis in this Chapter is particularly useful for the purposes of this study.

The chapter starts (6.2) with some general background to the regulation of communications network providers. More specifically, the notions of common carrier and universal access will be discussed, as well as the way in which these notions reflect the public interest in the governance of access to communications networks. The next section (6.3) will discuss the question about the general implications of the right to freedom of expression for the governance of access in the context of Internet access providers. Of specific concern is the question about the implications of the right to freedom of expression for the governance of horizontal conflicts over access between broadband providers and Internet users. Two different and conflicting views on these implications will be presented. The first view bases the protection of Internet access providers under the right to freedom of expression on the communicative liberties of Internet users and points to the possibility to regulate access providers in the interest of freedom of expression. The other view grants Internet access providers their own right to exercise editorial discretion over third party communications.

[336] See e.g. Lichtman & Posner 2005.

These general points of view will be illustrated in more detail by analyzing the way in which the right to freedom of expression has helped to shape the existing legal framework with regard to the responsibility of Internet access providers for illegal and unlawful third party communications (6.4). This framework consists of safe harbors for liability on the one hand, and the self-regulatory paradigm on the other hand. In the section 6.5, the legal governance related to filtering by access providers will be addressed. Internet filters have been consistently promoted as a way to restrict illegal information flows on the Internet. In the debate about Internet filters, concerns over the right to freedom of expression have played a prominent role.

In this chapter, the non-legal term Internet Service Provider (ISP) will be used to denote the basic Internet related services, such as Internet access, transmission and hosting. This chapter focuses almost exclusively on ISP activity that consists of providing access to the Internet for end-users (Internet access providers). Of special relevance is the legal status of ISP activity that goes beyond mere conduit and interferes at the level of content. The role of access providers is somewhat shifting in this regard, in the direction of more and more involvement, because of a complex interplay of economic, legal and technological developments. This chapter is not concerned with the precise scope of various legal provisions, e.g. the hosting or mere conduit safe harbors in the Directive on Electronic Commerce or the Digital Millennium Copyright Act, or the definition of electronic communications networks and services. Instead, the focus is placed on the way these provisions and the regulatory framework applying to the involvement of access providers with content and third party communications, have been shaped by restrictions by or concerns over the right to freedom of communication.

The nature of online communications means one has to consider the possible ramifications of Article 8 ECHR, which protects the right to private life and correspondence, or similar constitutional safeguards.[337] Notably, restrictions on into communications can run into the protection of both Article 8 and 10 ECHR. [338] There are similar (but different) safeguards under the United States constitution, such as the Fourth Amendment. First Amendment doctrine contains some elements relating to the private sphere as well. For instance, the impact of media on the private sphere of individuals can have an impact on the protection under the First Amendment.[339] Regulation may be permissible if it protects citizens against unwanted exposure to indecent communications in their private sphere.[340]The mere possession of indecent and even obscene material cannot be punished because of their private

[337] ECtHR 25 March 1983, *Silver and others v. the United Kingdom*, § 85 ("the two provisions overlap as regards freedom of expression through correspondence"). See also ECtHR 25 November 1997, *Grigoriadis v. Greece* (The punishment of a soldier for his utterances in a letter to a superior that was not disseminated more widely constitutes a breach of Article 10. The Court holds that the non-public nature of the utterances weighed against the necessity of the punishment.).

[338] ECtHR 21 February 1975, *Golder v. U.K.*

[339] Some courts have concluded that the First and Fourth Amendment are exclusive. See e.g. *ACLU v. NSA*, 493 F.3d 644 (6th Cir. 2007). See also Richards 2008, note 94.

[340] See e.g. *Rowan v. Post Office Dept*., 397 U.S. 728 (1970) (The law may grant addressees "*a mailer's right to communicate must stop at the mailbox of an unreceptive addressee*", citing "*the ancient concept that "a man's home is his castle*" into which "*not even the king may enter*"); *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978) (Indecency regulation of broadcast media – FCC declaratory order with regard to the 7 indecent words - constitutional because these media "*have established a uniquely pervasive presence in the lives of all Americans.*").

nature.[341] To restrict the scope of the analysis, the implications of the right to private life and the confidentiality of communications will not be addressed in detail. Sometimes, the term 'freedom of communication' will be used to refer to the communicative freedoms in the context of the Internet, including the right to respect for private life and the confidentiality of private communications. This is in line with the terminology used in this context in the Council of Europe Committee of Ministers, Declaration on freedom of communication on the Internet.

6.2 Regulation of communications network providers and freedom of expression

6.2.1. Background

The freedom to deploy and use communications networks is essential for the exercise of the right to freedom of expression and the freedom of communication more generally. The ability to receive and impart information and ideas has always to a considerable extent depended on effective carriage across different communications networks. Recognizing the enormous public utility of communications networks, states have established and facilitated postal services, telephony, telegraphy and electronic communication networks such as the Internet. On the other hand, throughout history, states have controlled, used or called upon communication network providers to suppress access to information and particular modes of distribution. Postal services[342], telegraph[343] and telephone companies,[344] and more recently Internet Service Providers (ISPs)[345] have been asked or put under legal obligations to ban

[341] See e.g. *Stanley v. Georgia* 394 U.S. 557 (1969) ("*obscenity statute is unconstitutional insofar as it punishes mere private possession of obscene matter*"). The implications of Stanley for restrictions on distribution are limited: *United States v. Reidel*, 402 U.S. 351 (1971) (Stanley does not imply a right to deliver or distribute the obscene material whose mere private possession cannot be constitutionally be penalized under Stanley*), Osbourne v. Ohio*, 495 U.S. 103 (1990) (holding that Stanley is inapplicable to criminalization of possession of child pornography, because the underlying rationale was found not to be paternalistic but aims to prevent actual harm to children).

[342] For the United States postal context, see generally, See John 1998; Fowler 1977; Deutsch 1938. The Supreme Court has ruled several times on the discretionary power of Congress to restrict access to the postal services. See e.g. *Ex Parte Jackson*; 96 U. S. 727 (1878); *Public Clearing House v. Coyne*, 194 U.S. 497 (1904) ("*Congress may designate what may be carried in, and what excluded from, the mails, and the exclusion of articles equally prohibited to all does not deny to the owners thereof any of their constitutional rights.*"); *Milwaukee Social Democratic Pub. Co. v. Burleson*, 255 U.S. 407 (1921) (The order of Postmaster General revoking second class mail privilege for newspaper due to repeated publication of nonmailable matter is constitutional); *Leach v. Carlile*, 258 U.S. 138 (1922) (Postmaster General granted considerable discretion to conclude whether material in the mail is postal fraud, i.e. overstated advertising of medicinal preparation); *Lamont v. Postmaster General*, 381 U.S. 301 (1965) (Scheme involving the delay of delivery of foreign publication, the Peking Press, until addressee reacts on notice, "*is unconstitutional, since it imposes on the addressee an affirmative obligation which amounts to an unconstitutional limitation of his rights under the First Amendment.*"); *Blount v. Rizzi*, 400 U.S. 410 (1971) (administrative censorship scheme for the postal mail violates the First Amendment since "*it lacks adequate safeguards against undue inhibition of protected expression*".). See also Justice Learned Hand's famous test for incitement in *Masses Publishing Co. v. Patten*, 244 F. 535 (S.D.N.Y. 1917) (concluding that the refusal of the Postmaster General to carry a revolutionary journal violated the First Amendment.).

[343] Western Union reportedly used to cut off certain newspapers (thereby running them out of business) if they would criticize the telegraph company or its business partner, the Associated Press. See e.g. Czitrom 1982, p. 26-28.

[344] See e.g. De Sola Pool 1983, p. 106. Typically, Information services over telephone are regulated to restrict access to certain content such as indecency. For the Dutch context, see Hoge Raad 26 Februari 1999, *Antelecom* (Conceptualizing a restriction on the possibility to use certain call-back services by the Antillian telecommunications monopolist as an interference with Article 10 ECHR.).

[345] See e.g. ECJ, Conclusions of Advocate General M. Pedro Cruz Villalón, 14 April 2011, Case C-70/10 (*Scarlet v. SABAM*).

certain communications from their networks. In other cases, communication networks have acted voluntarily, to restrict access and block and filter out information flows they did not wish to carry.[346]

Restrictions on carriage of content over communications networks raise issues under the right to freedom of communication. Restrictions on the newspaper's use of telegraphy, or the stipulation of special postal and tax rates for the press are examples of how restrictions and regulation of communication networks can undermine free public debate. More recently, concerns about freedom of communication on the Internet have arisen in the context of filtering by Internet Service Providers (ISPs) and the disconnection of Internet users from the network as a sanction for alleged copyright infringement.[347]

In contrast to the regulatory framework for the press, with its emphasis on non-interference and self-regulation, the regulation of postal services, telegraphy, telephony and electronic communication networks has been extensive. However, such regulation was traditionally mostly content neutral.[348] In Europe, the classical transport and communications services were nationalized relatively soon after the societal adoption of the underlying technologies. In the United States, the postal services are organized by the state due to the constitution, whereas telephony and telegraphy were always privately owned, but regulated industries.[349]

6.2.2. Regulation: rationales, universal service and common carriage

The extensive regulation of communication networks, which continues today, is informed by their general public interest on the one hand and legitimized by their particular economics - economies of scale and network effects - on the other hand. The market for communications networks brings about interconnection issues and the infrastructure tends to be an essential facility. In addition, regulation of communications networks contains elements of consumer and privacy protection. This chapter will not focus on these general characteristics of the regulatory framework for communications service providers but look more closely at a number of specific issues relating to the role of the right to freedom of communications in the regulatory framework and the ongoing discussions about the proper responsibility of Internet access providers with regard to third party communications.

Before looking more specific issues relating to freedom of expression and access providers, it is helpful to shortly address two central concepts in the regulatory framework for communications networks with regard to the governance of access, namely the 'universal service obligation' and 'common carriage'.

The 'universal service obligation' can be generally defined as a regulatory guarantee for all citizens to be able to get access to a service without discrimination – in particular regardless of geographic location –

[346] For examples see Nunziato 2009. See also Barron 1993.

[347] For a discussion of the disconnection of end-users by access providers and the right to freedom of expression, see United Nations 2011. See also Lucchi 2011.

[348] Telecommunications and postal regulation for national monopolies used to contain specific provisions for the stoppage or interruption of communications. See e.g. Article 14 of the (former) Dutch Telegraphy and Telephony Act 1904. The justification of this Dutch provision was found in the obligation for civil servants to report criminal acts when they become aware of them.

[349] U.S. Constitution, Section 8: Powers of Congress*: "The Congress shall have Power [...] To establish Post Offices and Post Roads*."

and with certain guarantees of basic quality.[350] United States law contains a universal service obligation in the telecommunications act 1996, 47 U.S. section 254. The European Union's Universal Service Directive, which is part of the regulatory framework for the electronic communications network and services, contains universal service obligations in Chapter II.[351] Currently, fixed telephony is a universal service – Article 4 (1) of the Universal Services Directive – and specific minimal guarantees as regards quality, capabilities and price are prescribed. Notably, the object of the universal service obligation is dynamic, as can be seen from the provisions themselves. The European Commission regularly reviews what should be considered part of the universal service obligation. In line with this dynamic interpretation, there is currently a debate whether or not end-user access to Internet broadband should be included in the universal service obligation.

The legal concept of 'common carriage' can be traced as far back as Roman law. It was developed further in English common law and became an important part of the United States common law system relating to transportation and communications services. In the 20th Century, the common carrier obligations were included in the administrative legal frameworks for communications network providers.

Common carriage can be seen as a distinctive regulatory model for service providers in the information and communications environment, distinctive from the model for the press and the broadcasting model. It applies to communications service providers, offering transmission or conduit services to the public. Common carriage ties access and equal treatment obligations to transportation and communications service providers invested with the public interest. Importantly, common carriage also implies a limitation on liability.[352] The common carriage requirement of non-interference and non-discrimination is usually understood only to apply to lawful communications.

Due to the rise of the Internet as the dominant communications network and the multiplicity of roles of the Internet in the networked communications environment (convergence), the discussion about the proper application of the 'common carriage' model has become more complex. In the early 1990s, telecommunications law scholar Eli Noam aptly called the issue "*content interconnection in an intermedia environment*". [353] Lately, the discussion about common carriage in the Internet environment has mostly taken place under a new flag, namely the principle of 'net neutrality'. Net neutrality refers to the principle of non-interference of Internet service providers with the way the network is actually being used. Net neutrality is often defended with reference to the economic and public interest value of the so-called 'end-to-end principle' in the Internet's design.[354] The non-interference standard is discussed with regard to blocking or prioritization, in relation to content, destinations, applications and end-user equipment. Access providers carry communications of websites directed at the general public and facilitate private communications such as e-mail or voice communications. Audiovisual material, the mass distribution of which is historically governed by broadcasting regulation, is flowing over the

[350] On the (history of the) notion of 'universal service' in the U.S. context, see Mueller 1997.

[351] Council Directive 2002/22, 2002 O.J. (L 108), 51 (EC).

[352] For the U.S. context, see e.g. Perrit 1992; Nuziato 2009; Barron 1993. See also Koelman 2000, note 165 cited references.

[353] See Noam 1992, pp. 426-28. See also Barron 1993.

[354] See Wu 2003. See also Van Schewick 2010.

Internet in unprecedented quantities as well. In other words, access providers carry one-to-one, one-to-many, and many-to-many types of communications at the same time. They are the new gateways to online media and basic information services. In addition, broadband services facilitate the use of user-driven software applications, such as peer-to-peer filesharing, Internet telephony and e-mail.

Although it may seem logical to see a link between the role of the state to promote the effective exercise of one's right to freedom of communication on the one hand and the existence of common carrier and universal service obligations on the other hand, this link is not always made by regulators in practice. In fact, historically, the link between these fundamental regulatory concepts for communications regulation and the right to freedom of expression and democratic and societal participation more generally was not made at all and has only quite recently been made in the United States during the Clinton's administration and later in the European context. The European Commission now links universal service obligations to the question whether the respective services (and service levels) are essential for *social inclusion*.[355] It is clear that the effective basic communicative freedoms can be considered a prerequisite for social inclusion as well. A more explicit link between freedom of communication and a fundamental right to Internet access has recently been made in the context of proposals to disconnect users from the Internet. The link between freedom of communications and common carriage types of obligation is typically made in the context of restrictions by ISPs on access to content through filtering technology, not controlled by the end-user.[356]

6.3 Freedom of expression and Internet access providers

6.3.1 Status of Internet access providers under the right to freedom of expression

From the perspective of Article 10 ECHR access providers can claim protection under the right to freedom of expression in cases where public authorities would prevent them from offering their services on the market, or oblige them to block or filter content. In *Autronic*, in which the Court first clarified that also companies enjoy protection under Article 10 ECHR, the Court concluded that

> "*Article 10 […] applies not only to the content of information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information.*"[357]

Thus, Internet access providers can claim protection under Article 10 ECHR for interferences (in vertical relations) with their role in transmitting information and ideas, irrespective of the actual content. Interferences would have to satisfy the test of Article 10, second paragraph. As can be seen from the citation above, the interference with the means of transmission and reception offered by communications providers is derived from the interests of others to impart and receive information and ideas freely. Notably, it also follows from the ECtHR's case law that users of communications services can sometimes themselves complain against restrictions (at least by public authorities) on the use of

[355] EC, Universal Service, http://ec.europa.eu/information_society/policy/ecomm/current/consumer_rights/universal_service.
[356] See Section 6.5.
[357] ECtHR 22 May 1990, *Autronic v. Switzerland*. See also ECtHR 24 May 1988 *Mueller and others v. Switzerland*.

such means which affect them directly.[358] Notably, the requirement that restrictions have to affect applicants to the Court directly delineates this possibility to claim protection under Article 10 ECHR, from an *actio pupolaris*.

6.3.2. Access regulation and the right to freedom of expression

The most difficult questions about the implications of the right to freedom of expression for the legal governance of access in electronic communications networks arise in the context of horizontal relations between communications service providers and the users of the network. First, does the right to freedom of expression impact on the legal governance of horizontal conflicts over access? What is the proper role of the state is in this regard? If, all of a sudden, all access providers would decide to block access to a certain controversial but legal website, would this information provider have to be able to complain about this due to its right to freedom of expression protected by Article 10 ECHR? And, more generally, does the right to freedom of expression point to a role for public authorities to prevent access providers from exercising undue interference with communications on the network? As will become clear in this chapter, the views on this issue diverge and there may not be a generally accepted set of implications of the right to freedom of expression to answer these questions. Below, a general overview of the debate will be offered by contrasting two generalized points of view.

One point of view would consider the protection of access providers under the right to freedom of expression to be derived from the communicative liberties of end-users.[359] This view would hold that Internet access providers can claim protection under the right to freedom of expression to the extent that they can base their claim on the interests of their users to impart and receive information and ideas freely. Notably, this line of thought directly implies that it is possible for access providers to act in conflict with the communicative interests of their users. In other words, this view could inform the State to consider regulating access providers to guarantee the protection of these interests through legal requirements.[360] Some would go further and claim that the state has a proper legal obligation to restrict access providers from interfering with the free flow of information on their networks. In the European context this positive obligation on the State can be linked to the positive obligation on the state to promote pluralism and the role of the state to protect the *effective exercise* of the right to freedom of expression.[361]

The other point of view, which is mostly found in the United States, does not make the connection between the protection of access providers under the right to freedom of expression and the rights and freedoms of the users of the network. Instead, it conceptualizes the right to freedom of expression as a negative right which prevents government from regulating the way in which the free exercise of the right to freedom of expression plays out in private relations. The right to freedom of expression protects legal entities and actual individuals alike. In this view, the right to freedom of expression protects the

[358] See e.g. ECtHR 29 October 1992, *Open Door v. Ireland*.

[359] See e.g. CoE, Committee of Ministers, 'Declaration on Freedom of communication on the Internet', 28 May 2003. See also Balkin 1990; Balkin 2004; Benkler 2001; Nunziato 2009; De Sola Pool 1983; Carter 1984; Barron 1993.

[360] See e.g. Berman & Weitzner 1995. See also Krattenmaker & Powe 1995.

[361] See Section 4.4.1.

discretion over communicative means that a particular entity controls, be it a natural person, the owner of a nation-wide broadband network or an online news outlet.[362] This protection would be granted in vertical relations against regulation and government interference. With regard to horizontal conflicts over access, the right to freedom of expression would simply require that government would leave the resolution to the functioning of the market. Hence, this view denies the possibility of government to be positively involved in the protection of freedom of expression in society, since freedom of expression is both seen as a negative constraint on government involvement as well as not restricted to proper individuals.

These two different points of view and their implications for the status of access regulation under the right to freedom of expression can be illustrated by contrasting the status of 'common carriage' with the status of access regulation for the press. Common carriage can be seen as the strongest possible form of access regulation. It basically nullifies the editorial freedom of the entities it is applied to and would, as a result, be incompatible with the right to freedom of expression if applied to the press. As discussed in Chapter 5, the editorial freedom of the press, is partly informed by the public interest and the communicative interests of the public and possible speakers. It also protects the press, as a speaker, in relation to possible interferences by public authorities to promote the communicative interests of users and possible speakers.

In the context of traditional conduits, such as the postal services and telephony, the public interest is typically considered to entail universal access, and indiscriminate and non-interference with communications. Common carriage obligations, which were explicitly based on these public interests, ensured that communications services were acting in this public interest. As pointed out above, universal access and common carriage, amongst other regulatory requirements, ensure the widest possible exercise of communicative liberties by Internet users.

Now the question is to what extent access providers, like the press, assert a right to freedom of expression to defend a possible decision to restrict certain information flows on their networks?[363] There are two contexts in which one could imagine such claims to be made: vertically, in the context of common carrier obligations and horizontally, with respect to access claims by possible users of their networks in reaction to voluntary decisions to restrict information flows for instance through blocking and filtering.

The case law of the European Court of Human Rights does not resolve whether Article 10 ECHR protects the decision of the owner of a communications network *not to* use those means for certain communications. Under Article 10 there is a right to remain silent,[364] but it is highly questionable whether this right – that has been construed in specific circumstances relating to individual liberty – would apply to a corporate entity that merely provides the means to communicate. The fact that Article 10 ECHR applies to individuals and corporations alike could be used to argue that the right not to

[362] See e.g. Yoo 2010. See also Tribe & Goldstein 2009.

[363] One of the reasons I ask this question is because of developments under United States First Amendment doctrine, which increasingly point to a positive answer to this question.

[364] See Van Dijk et al 2006, p. 783.

communicate – in the case of conduits, the right *not to transmit* – is also protected by Article 10 ECHR. However, it is unlikely that the Court would be willing to come to this conclusion.

It is more likely that the Court would respond to horizontal access issues under the right to freedom of expression between access providers and users of the network, by balancing the interest of the free exercise of the right to freedom of expression of users on the one hand, with the right to the free exercise of the provider's property on the other hand. An access provider's right *not to transmit* third party communications would be based on the economic freedom of communications service providers.[365] This freedom is not necessarily less protected than the freedom of communication of end-users.[366]

The ECtHR had to deal with a comparable issue involving restrictions on the use of private property for expressive purposes in the case *Appleby* and it did not refer to any right not to speak in this case. The decision to refuse access for expressive purposes was considered to be based on the economic freedom of the owner of the means of communication, not on its freedom not to use those means for the expressive purposes of applicants, sanctioned by the right to freedom of expression.[367] In *Appleby*, the ECtHR took account of the Supreme Court's jurisprudence on access to a private forum to speak and protest[368] and concluded that "*while freedom of expression is an important right, it is not unlimited. [...] Regard must also be had to the property rights of the owner of the shopping center under Article 1 of Protocol No. 1."*[369] The Court concluded that Article 10 ECHR "*does not bestow any freedom of forum for the exercise of that right. While it is true that demographic, social, economic and technological developments are changing the ways in which people move around and come into contact with each other, the Court is not persuaded that this requires the automatic creation of rights of entry to private property, or even, necessarily, to all publicly owned property […]."* In other words, under the Convention there is no such thing as a right to access private property to effectively impart ideas. The Court left room for an exception if "*the bar on access to property has the effect of preventing any effective exercise of freedom of expression or it can be said that the essence of the right has been destroyed."* In such cases, "*a positive obligation could arise for the State to protect the enjoyment of the Convention rights by regulating property rights." Notably,* the Court explicitly referred to Marsh *v.* Alabama, the U.S. Supreme Court's judgment affirming speech rights in a corporate town, as an example of such circumstances.[370]

6.3.2 First Amendment

Like Article 10 ECHR, the First Amendment not only protects the freedom of speech or of the press, but also the freedom to receive and distribute information and ideas.[371] There is a rich history of case law

[365] For example in the Netherlands, see Hoge Raad [Dutch Supreme Court] 12 maart 2004, (*XS4all/Abfab*).
[366] This could be different in the United States.
[367] See ECtHR 6 May 2003, Appleby and Others, §. 43.
[368] Id., §7.
[369] Id., § 43.
[370] Id., § 47.
[371] *Griswold v. Connecticut*, 381 U.S. 479 (1965). See also Section 5.5.1.

relating to the constitutionality of the publicly owned postal services under the First Amendment dealing with restrictions on the ability to have information distributed or to receive it freely through the mail.[372] Privately owned communications networks can assert the protection of the First Amendment against state actions restricting the free flow of communications on their networks. It is worth noting that the distribution of unprotected material, such as obscenity, is itself not protected by the First Amendment.[373] However, regulations targeting unprotected speech are still scrutinized for their effects on constitutionally protected communications.[374]

The First Amendment, as applied by U.S. Courts today, arguably implies a broader right not to speak than freedom of expression in the European context.[375] This right has been argued to be available to the owners of the means of communications such as broadcasters, cable companies and Internet access providers.[376] Thus the owner of the means of communication would receive protection of the First Amendment against restrictions (not) to use their property for certain speech, on top of the constitutional protection of their property rights.[377] As mentioned above, this theory equates the exercise of the right to freedom of expression to a considerable extent with the exclusive right over the use of one's property. Property distribution, including the ownership of communicative means, is taken for granted and is its use for communicative means is considered in line with the free market place of information and ideas.

Although in the United States, the constitutional law mainstream is open to this view, and increasingly, the Supreme Court's First Amendment doctrine seems to support it, it is not generally accepted and remains controversial. One of the main lines of criticism stresses the incompatibility of this view with the ideal of individual liberty and autonomy underlying the right to freedom of expression, as well as democratic ideal of self-governance.[378] From the ideal of democracy, access providers and the entities that merely act as the gateways to public debate more generally should be prevented from exercising undue interference with the public network information environment. Arguably, the right not to speak only plays a role in cases of compelled speech involving individual liberty. It's the intellectual freedom of individuals that is worthy of protection against compelled speech.

Another way of looking at the question about the legitimacy of interferences of access providers that would harm the communicative liberties of end-users and information providers is to take as a starting point that the 'normal' practice for ISPs would be to provide access to all. General obligations not to do something, namely restrict access to certain users of a communication network, should be distinguished from obligations to use the networks for particular expressive purposes. The United States common law

[372] See Section 6.2.1.

[373] *United States v. Reidel*, 402 U.S. 351 (1971).

[374] See e.g. *New York Times Co. v. Sullivan, 376 U.S. 254 (1964)*; *Smith v. California*, 361 U.S. 147 (1959).

[375] See e.g. *West Virginia State Board of Education v. Barnette*, 319 U.S. 624 (1943) (State law that requires all children to salute to the flag unconstitutional; distinguished in *Pruneyard*.) *Wooley v. Maynard*, 430 U.S. 705 (1977) (law punishing covering up of motto Live free or die on New Hampshire license plate unconstitutional.) See also H*arper & Row Publishers, Inc. v. Nation Enters*, 471 U.S. 539, 559 (1985).

[376] See Balkin 2004, pp. 17-21. See also Benkler 2001; Chandler 2008; Seidman 2008.

[377] Property rights are protected by the Fifth Amendment and Fourteenth Amendment.

[378] See e.g. Baker 1994.

theory as regards common carriers functioned in this way.[379] The communications service provider, through its manifestation to the public, 'chose' whether it was a conduit or a publisher. If it opted for the conduit option, it would have no First Amendment rights itself, in terms of the ability to control and discriminate between communications and different sources. If it opted for a publisher status, it would get its own First Amendment rights.[380] Notably, this choice also had an impact on third party liability standards for the service provider. Common carriers received tort immunity in return for equal access obligations, whereas entities that exercised editorial discretion could be held accountable. Interestingly, in the United States, these tort standards no longer govern the behavior of Internet intermediaries, as will be shown below.

6.4 ISP intermediary liability and the right to freedom of expression

6.4.1 Background

The debate about the responsibility of ISPs for their role in providing access to the Internet started in the 1990s in two different legal contexts, namely content regulation on the one hand, and the protection of intellectual property rights on the other hand. Traditional content regulation focusing on publishers and the mass media and the enforcement of national laws were becoming problematic, unfeasible, and unpractical in the context the Internet, since many new information providers entered the public networked information environment and could reach global audiences from locations all over the world. A shift in focus led regulators, litigants and the creative industries to focus on the responsibility and possible role of different types of ISPs to enforce existing rules with regard to illegal and unlawful information flows.[381] In the absence of specific legislation for ISP responsibility, the question whether ISPs could and should be held liable for illegal and or harmful activities of end-users and online information providers and what could be expected of the different types of services in terms of policing the Internet and their users, wasn't easily answered.[382] The subsequent legal uncertainty that was the result of this first wave of litigation ran counter to the efforts to facilitate e-commerce and the development of the Internet and the Web more generally. This led legislatures in the U.S. and Europe to enact specific rules about the legal responsibility of ISPs.[383]

The regulatory response with regard to ISP responsibility had two interdependent branches. On the one hand, so-called safe harbors for Internet and online intermediaries were introduces into the law, first in the U.S. and several European countries, and later also at the level of the European Union.[384] These safe

[379] See Perrit 1992, pp. 66-67. Perrit warns that these conclusions are far from clear. See also Barron 1993.

[380] See Perrit 1992.

[381] Early examples of the targeting of Internet access providers by public authorities can be found in Germany. In a case involving the accessibility of child pornography on Compuserve, the employee Felix Somm was convicted by a Court in Munich and CompuServe was ordered to block the material for German subscribers. In another case, involving the radical-left online publication 'Radikal' hosted in the Netherlands, prosecutors threatened to prosecute Internet access providers if they would fail to block the allegedly terrorist material for their users in Germany. See e.g. European Commission 1996b, p. 15.

[382] For a discussion of access to communications networks, tort liability principles and the right to freedom of expression, for the European context, see Koelman 2000 and for the United States, see Perrit 1992.

[383] For a discussion and legal comparison of the two frameworks, see Koelman 2000.

[384] A number of Member States, including Sweden and Germany had already introduced safe harbours at the national level before the EU harmonized intermediary liability for ISPs.

harbors were to provide legal certainty for ISPs and establish the proper boundaries of ISP liability for the illegal or infringing activities of third parties.

On the other hand, legislatures called for further self-regulation and a continuing dialogue between the various stakeholders. In other words, the safe harbor regulation established the legal boundaries with regard to the responsibility of Internet intermediaries in the law. Within these boundaries, the industry was expected to establish self-regulatory practices to help to address the circulation of unlawful, infringing and also harmful communications. This second branch of the regulatory response, namely self- and co-regulation, became a new paradigm for dealing with information flows on the Internet. Self-regulation was argued to be a better way to reach public policy goals than command and control types of regulation. [385]

The self-regulatory paradigm for ISPs and information services more generally was first established in the EU with the 1998 Council Recommendation for the European audiovisual and information services industry.[386] The 1998 Council Recommendation calls upon the Member States to promote, at the national level, the voluntary establishment of self-regulatory frameworks for the protection of minors and human dignity on the Internet. In the United States, maybe the best example of the self-regulatory paradigm is one of the limited liability provisions itself, namely CDA, Section 230.[387]

Both the self-regulatory paradigm and the drafting of liability standards lead to concerns over the right to freedom of expression, which will be discussed in this section. First, the liability standards for Internet intermediaries are directly related to the possible chilling effects of these standards on online information flows. Too weak a standard would incentivize Internet intermediaries to be more restrictive and possibly too restrictive, thereby obstructing legitimate information flows in the networked information environment.

Second, Internet content self-regulation was directly meant to result in the removal, filtering and blocking of information by the industry. Of specific concern are the possible effects of self-regulation on legitimate content flows and the lack of substantive and procedural safeguards. The question arises whether overly restrictive practices by access providers, resulting from self-regulation, are in line with the right to freedom of communication and to what extent the state itself can be held accountable in its role of promoting, cooperating and shaping self-regulatory frameworks for content regulation on the Internet.[388]

6.4.2 Intermediary liability: EU and the U.S

[385] See Price & Verhulst 2005, pp. 135-162. See also Hans-Bredow Institut 2006. Self-regulation has long been promoted beyond the context of Internet regulation. See Baldwin & Cave 1999.

[386] Council Recommendation 98/560, 1998 O.J. (L 270), 48 (EC).

[387] See Section 6.4.4.

[388] See Tambini et al 2008. See also Kreimer 2006; Bambauer 2011.

The European legal developments with regard to ISP liability and responsibility took place in the context of illegal and harmful content on the Internet and the protection of minors on the one hand,[389] and the enforcement of copyright law on the Internet on the other hand.[390] These two perspectives met in the discussion leading to the Directive on Electronic Commerce (ECD).[391] The ECD contains provisions which state that basic Internet intermediaries are under certain conditions not to be held liable for the information flows they facilitate. This framework of limited liability consists of three horizontal liability exemptions in the ECD (Article 12-14), as well as ban on preventive monitoring obligations for these types of intermediaries (Article 15).[392] To be more precise, the Directive protects information society services[393] acting as intermediaries for their 'mere conduit' (Article 12), 'caching' (Article 13), and 'hosting' (Article 14) activities. Article 15 prevents the Member States from imposing general obligations on the providers of the services falling under any of the safe harbors to monitor the information that they transmit or store, or to seek facts or circumstances indicating illegal activity.

An Information society service acting as mere conduit, such as an Internet access provider connecting end-users to the Internet, is protected under Article 12 ECD if it does not initiate the transmission, select the receiver of the transmission, or select or modify the information contained in the transmission. Under Articles 13 and 14 ECD, the proxy caching and hosting activities of information society services are conditionally exempted from liability. Notably, the safe harbors do not affect the possibility to claim injunctive relief. They explicitly leave open the possibility for a court or administrative authority to require an ISP to terminate or prevent an infringement. This also applies to information society services acting as mere conduits. Moreover, exemptions do not affect the lawfulness of the processing of information by providers of any of these types of intermediary services. The lawfulness has to be determined by applying the relevant laws of the Member States.[394] Hence, the exemptions do not protect the providers of exempted services against litigation which is aimed at an injunction. Although controversial, judges have ordered Internet access providers to disconnect a specific end-user or to block access to specific online information.[395]

[389] See in particular European Commission 1996b; European Commission 1996c; Council Recommendation 98/560, 1998 O.J. (L 270), 48 (EC); European Parliament and Council Recommendation, 2006/952, 2006 O.J. (L 378), 72 (EC). See also European Commission 1997b, p. 5 ("*in the absence of an accepted classification of operators and functions, the question of liability for operators who merely provide access to services or communications networks remains open. However, a majority came out in favour of an absence of liability for these operators, which however does not me that they have no role to play, for example in informing consumers.*").

[390] See European Commission 1995; European Commission 1996a.

[391] European Commission 1997a; European Union Ministers 1997, and the Directive on Electronic Commerce (ECD): Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC).

[392] Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC).

[393] Article 2 sub a ECD refers to Article 1 (2) Directive 98/34/EC as amended by Directive 98/48/EC for a definition of 'information society service': "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".

[394] In civil law terms, the safe harbours do not affect the lawfulness of certain actions but they harmonize the requirements for finding fault and or negligence. See Koelman 2000, p. 52.

[395] See e.g. Chavannes 2007, pp. 174-178. See also Jakobsen 2010.

In the United States, the liability of Internet intermediaries for copyright infringements and the responsibility for illegal content such as indecency or defamation has been dealt with separately. The fragmentation of safe harbors along the lines of different underlying legal concerns, which is called a vertical approach, is one of the main differences with the European framework of Internet safe harbors, which has adopted a horizontal solution. The Digital Millennium Copyright Act introduced a safe harbor for liability of access providers for copyright infringement in Section 512 (a). It provides that no general monitoring obligations can be imposed upon access providers. Injunctive relief with regard to possible copyright infringement by access providers is further restricted to orders blocking access to subscribers or orders to block access, to a specific, identified, online location outside the United States.[396] An intermediary liability exemption for defamation and other illegal content, except for criminal law, intellectual property law, and communications privacy law, can be found in CDA, Section 230. This provision, introduced by the Communications Decency Act in 1996, restricts the liability of so-called interactive computer services. Courts have interpreted it as an absolute safe harbor for ISPs with regard to third party content. In the next section, the legal developments that led to the current liability regime based on CDA, Section 230 will be discussed in detail, as they are intrinsically linked to the implications of the First Amendment for speech carrying intermediaries and the distinction in First Amendment doctrine between different types of speech intermediaries.[397] Another difference between United States and the European law, is the scope of the safe harbor framework. The safe harbors in the DMCA, section 512, and the CDA, section 230, both extent to third party liability of search engines, whereas the European framework did not include this type of service. We will address this difference in more detail in Chapter 9.[398]

The Council of Europe and its Committee of Ministers have addressed ISP responsibility in a number of legal instruments, the most important of which are the Convention on Cybercrime, the Recommendation on self-regulation concerning cyber content, the Declaration on Freedom of communication on the Internet and the Recommendation on freedom of expression and information with regard to Internet filters.[399] The Recommendation on freedom of expression and information with regard to Internet filters will be addressed in more detail in section 6.5.

As will become clear shortly, the safe harbors and the self-regulatory framework for ISPs, take into account freedom of expression concerns. Below we will address the way in which this has happened in more detail. As the safe harbors in the ECD were inspired by similar legislation in the United States, ISP liability regulation in the U.S. will be addressed first.

6.4.3 The DMCA safe harbors and the First Amendment

[396] Section 512 (j)(1)(B) of the U.S. Copyright Act. Notably, this restriction on possible injunctions is absent in the final text of the Directive on Electronic Commerce. For a discussion, see Koelman 2000.

[397] See Freiwald 2001; Cannon 1996; Myerson 1995.

[398] See Section 9.3.

[399] CoE, Convention on Cybercrime, 2001; CoE, Committee of Ministers, Recommendation Rec(2001)8 of the Committee of Ministers to Member States on self-regulation concerning cyber content, 2001; CoE, Freedom of communication on the Internet, 2003; CoE, Committee of Ministers, Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters, 2008.

Before going into detail it is worth noting that the First Amendment applies differently in the context of intermediary liability for copyright infringement and other unlawful activity in the United States.[400] In copyright cases U.S. courts usually refuse to admit a separate freedom of expression defense, since free speech concerns are considered to be internalized into copyright law itself and copyright law is content neutral.[401] In cases of liability for defamation and otherwise illegal content, the Courts have always needed to balance restrictions on free speech and distributor liability with the requirements of the First Amendment, which sets limitations on liability standards of distributors.[402]

The DMCA safe harbors clarify the responsibility of online intermediaries with regard to third party copyright infringements. In particular, the due process guarantees tied to the elaborate provision with regard to notice and takedown for hosting providers can be seen to be informed by freedom of expression concerns. A hosting provider has to notify their customers if they decide to remove or disable access to material (Section 512 (g)(2)). In addition, the DMCA contains a disincentive to issue unjust notifications of infringement. It is unclear to what extent these guarantees were *necessary* from the perspective of the First Amendment. As mentioned above, unlike in the case of distributor liability for defamation, references to the First Amendment in copyright infringement cases are rare. The *Netcom* case, a case before the adoption of the DMCA safe harbors about the responsibility of the provider of a BBS for copyright infringements by its users, contains such a reference. The First Amendment plays a role in the consideration of the fair use defense.[403]

Those protected by the DMCA safe harbors do have to implement a policy that provides for the termination of access of repeat infringers.[404] Nimmer concludes that one can only be considered a repeat infringer - in contrast to an *alleged* repeated infringer - when there is actual proof of infringements in multiple occasions. Hence, a reasonable policy for a broadband provider can place be relatively strict requirements on what is needed before it terminates an Internet subscription. Intermediaries also have to accommodate and not interfere with standard technical measures to prevent infringements from taking place, which is a reference to the anticipated improvements in filtering technology. The DMCA allows and expects ISPs to disable access to material or activity claimed to be infringing as long as it acts in good faith in response to a claim or based on facts of circumstances

[400] Koelman 2000, pp. 42-44.

[401] See generally Hugenholtz 2001. See also Stone et al 2008, p. 504. For the relation between the First Amendment and Copyright law, see *Eldred v. Ashcroft*, 537 U.S. 186 (2003) (upholding copyright term extension and concluding that copyright law internalizes First Amendment concerns in idea expression dichotomy and availability of fair use defense.).

[402] See Myerson 1995.

[403] See *Religious Technology Center v. Netcom*, 907 F. Supp. 1361 (N.D. Cal. 1995). See also Koelman 2000, p. 41.

[404] See Nimmer & Nimmer looseleaf, § 12B.10. Nimmer does not discuss the communicative interests of subscribers not to have a subscription terminated. U.S. courts have held that service providers do not have to implement privacy invasive policies to ensure the impossibility of continuation of service (in the context of free email services) of the repeat infringer. See *Io Group v. Veoh Networks*, 586 F.Supp.2d 1132, 1145 (N.D. Cal. 2008) ("*[S]ection 512(i) does not require service providers to track users in a particular way or to affirmatively police users [...]").* The provision's reference to account holders or customers raises the question what intermediaries such as search engines should do with repeat infringers they do not have a contractual relationship with. See also Ginsberg 2008, note 81 and accompanying text.

that the material or activity is infringing (512 (g)(1)). Thus, Internet access providers could in fact decide to block access to certain material on the Internet they consider to be infringing.[405]

The DMCA safe harbors for ISPs have been shown to have a chilling effect on legitimate third party communications, in particular in the context of the hosting safe harbor and the safe harbor for information location tools (search engines).[406] There is - to my knowledge - no case law about the constitutionality under the First Amendment of the possible incentives the DMCA places on ISPs to block constitutionally protected speech or to disconnect users. The issue remains hotly debated, currently in the context of the proposal of a new bill relating to copyright enforcement online, the PROTECT IP ACT, which foresees DNS filtering by access providers of websites that contribute to copyright infringements.

6.4.4 Communications Decency Act 230 and the First Amendment

Outside of copyright law, in the areas of defamation and indecency regulation, the legal developments with regard to intermediary liability took quite another direction. In the 20th Century, United States legal practice had developed a rich body of case law dealing with publisher, distributor and carrier tort liability and the First Amendment.[407] A standard case for distributor liability under the First Amendment, for instance, is Smith v. California. The Supreme Court ruled that a law establishing strict liability for booksellers selling obscene material is unconstitutional, because it would inhibit freedom of expression by making booksellers reluctant to exercise it.[408] More in particular, the Court emphasized that strict liability on distributors would impose an unconstitutional restriction on the public's access to constitutionally protected material. As mentioned above, common carriers invested with the public interest received immunity for defamation and other torts in return for equal access obligations.[409]

The first ISP defamation cases in the nineties were dealt with, without the availability of specific rules for the liability of different kinds of Internet intermediaries. In *Cubby*, a New York district court determined that the provider of the bulletin board service CompuServe, should be viewed as "*the functional equivalent of a more traditional news vendor.*"[410] The Court considered several print analogies before coming to this conclusion. Even though CompuServe had the contractual right to refuse to carry a particular publication, "*in reality, once it does decide to carry a publication, it will have little or no*

[405] See also FCC's proposed standards relating to an open Internet, which include the statement that: "*[t]he draft rules would not prohibit broadband Internet access service providers from taking reasonable action to prevent the transfer of unlawful content, such as the unlawful distribution of copyrighted works*." See Federal Communications Commission 2009.

[406] See Berkman Center for Internet & Society, Chilling Effects Clearinghouse.

[407] For an overview, see Ardia 2010; Perrit 1992.

[408] *Smith v. California*, 361 U.S. 147 (1959) (arguing, with regard to the contents of an ordinance imposing liability on booksellers, that the absence of a requirement of knowledge of the contents of the book on the part of the seller implied that the ordinance would tend to impose a severe limitation on the public's access to constitutionally protected matter).

[409] See Ardia 2010, pp. 398-401. See also Perrit 1992. Perrit also explains that the precise contours of common carriage status on liability and First Amendment rights have become unclear due to fact that since a century common carriers had become heavily regulated industry, thereby pushing the common law standards for common carriers to the background in favour of administrative law. See also Perritt 2010, pp.436-460 (arguing for free market approach in combination with the development of common law standards through litigation as well as the combination of tort immunity and equal access obligations.).

[410] *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

editorial control over that publication's contents."[411] CompuServe had "*no more editorial control over such a publication than [...] a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so.*"[412] The Court subsequently established the distributor standard for an Internet intermediary like CompuServe to be liable for illegal content:; it would only be liable if it "*knew or had reason to know of the allegedly defamatory […] statements.*"[413] Hence, a passive, unknowing conduit would not be liable for unlawful third party communications.

In *Prodigy*,[414] the New York Supreme Court reversed the causal connection between editorial oversight and distributor liability and ruled that an online bulletin board operator is liable if it does exercise such control over the selection of content. Prodigy had been offering online bulletin boards, while actively removing messages it deemed offensive by using technical filtering products and content screening guidelines for its moderators. The *Prodigy* judgment was argued to be bad law, both by proponents of more robust protection of speech online and proponents of more effective regulation of illegal and harmful content. The former argued that if intermediaries like Prodigy were to be treated analogously to speakers in the print world, this would result in chilling effects on speech, since they would start to monitor and police all communications on their platforms. The latter argued that the Court should not punish the good faith efforts of intermediaries to combat illegal and harmful content by increasing their liability for material that would slip through. This would induce them to be more passive and do nothing about illegal and harmful content.

Acting on the concern that *Prodigy*'s liability standard could cause intermediaries not to assist in restricting access to illegal or harmful content, Congress overruled *Prodigy* and introduced a 'Good Samaritan' blocking and screening of offensive material exemption for Internet intermediaries in the Communications Decency Act.[415] CDA, Section 230 (c)(1) now 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.[416]

Moreover, CDA, Section 230 (c)(2) limits the civil liability of interactive computer services that do decide to restrict access or availability to content. It provides that:

> No provider or user of an interactive computer service shall be held liable on account of— (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make

[411] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).
[412] *Id.*
[413] For a discussion of *Cubby* and the different liability standards for publishers and distributors because of the First Amendment see Myerson 1995.
[414] *Stratton Oakmont, Inc. v. Prodigy Services Co.* No. 31063/94, 1995, WL 323710 (N.Y. Sup. Ct. May 1995).
[415] See Cannon 1996; See also Koelman 2000, p. 35.
[416] 47 U.S.C. § 230 (c)(1).

available to information content providers or others the technical means to restrict access to material described in paragraph (1).[417]

These provisions were primarily meant to remove possible incentives for online intermediaries not to remove or block access to certain information and to prevent claims against Internet filtering products.[418] In practice, CDA, Section 230, is most famous for having been interpreted by the Courts as an absolute safe harbor for hosting or providing access to third party defamation and indecency for a range of Internet intermediaries, including access providers, hosting providers, and search engines.[419]

Notably, the Communications Decency Act did more than introduce section 230. This provision started as a legislative side-note, but gained prominence while some of the CDA's core provisions were struck down on constitutional grounds. The main goal of the Act was to restrict the availability of indecent content on the Internet by making it illegal for information providers to provide access to obscene and indecent content to minors. This part of the Communications Decency Act was contested on First Amendment grounds and struck down by the Supreme Court in *ACLU v. Reno*.[420] The sequel to the CDA, i.e. Child Online Protection Act (COPA) was passed in 1998, was also struck down on constitutional grounds.[421] *Reno* is an important judgment since it (partly) answers the question about the constitutional protection for speech on the Internet. It establishes that Internet speech receives the highest possible protection under the First Amendment relative to other media, i.e. similar to the press.[422] Notably, a more extreme position, in terms of protection against government interference is possible. Some have argued in favor of no legal restrictions on content whatsoever because of the interactive nature of the Internet and the highly supportive features of the Internet in terms of self-governance by the users of the network.[423]

The most interesting aspect of the absolute safe harbor for Internet intermediaries in CDA, Section 230 for this discussion is that it gives Internet intermediaries, acting as distributors but also those acting as Internet access providers and search engines,[424] considerable discretion over third party communications. In fact, this provision is in many ways the opposite of a common carrier obligation. It legally permits Internet access providers to – in good faith – restrict access to or the availability of material that it considers to be "*otherwise objectionable, whether or not such material is constitutionally*

[417] 47 U.S.C. § 230 (2).

[418] See Tushnet 2008.

[419] See e.g. *Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997). For a discussion see Freiwald 2001.

[420] *Reno v. ACLU*, 521 U.S. 844 (1997).

[421] *ACLU v. Mukasey*, cert. denied (Sup Ct. Jan 21, 2009), *ACLU v. Mukasey*, No. 07-2539 (3d Cir. July 22, 2008); *Ashcroft v. ACLU*, 542 U.S. 656 (2004), 322 F.3d 240 (2003); *Ashcroft v. ACLU*, 535 U.S. 564 (2002), *ACLU v. Reno*, 217 F.3d 162 (Third Circuit 2000); *ACLU v. Reno*, 31 F. Supp. 2d 473 (ED Pa. 1999).

[422] *Reno v. ACLU*, 521 U.S. 844 (1997) (CDA provision 223 (a) and (d). The Court ruled that "*the risk of encountering indecent material [on the Internet] by accident is remote because a series of affirmative steps is required to access specific material*." The Court also considered the lack of precision and the subsequent burden on protected speech. And it considered that the legislation enacted was not the least restrictive means.

[423] See e.g. Berman & Weitzner 1995. See also *Sable Communications, Inc. v. FCC*, 492 U.S. 115 (1989) (Holding that the First Amendment bars federal statute prohibiting indecent telephone messages; Telephone must be distinguished from broadcasting because affirmative steps need be taken by the audience.) See also Barlow 1996.

[424] See Section 9.3.3.

protected."[425] Hence, it facilitates filtering at the network level by Internet access providers and expressly legitimates interferences with lawful content. On top of this, the first paragraph is an absolute defense against liability for providing access to unlawful material, sanctioning the decision to act as a passive mere conduit. In other words, in the digital era, the United States legislature granted the typical common carrier, i.e. the Internet access provider, tort immunity without corresponding equal access provisions.[426]

The legal discretion offered to ISPs by CDA Section 230 (c)(2) is also a reflection of the self-regulatory paradigm for Internet regulation. The service provider's choice between voluntary common carriage or restrictive access is left to the industry. The state places itself at a distance, providing the legal space for ISPs to act in and establish the market for information and communications services, within which they are allowed and expected to self-regulate in view of certain public interest objectives. The legislative history of the Communications Decency Act clearly shows that the U.S. legislature meant the Communications Decency Act to provide the space for ISPs to be restrictive, envisaging a role of suppressing objectionable information. In practice, it is mostly used to protect against liability for providing access to illegal material.[427]

But what can be said about the question in what way Section 230 of the CDA is linked to the First Amendment? More specifically, what do its enactment and survival tell about the dominant view of the implications of the First Amendment for access governance in horizontal relations between Internet access providers and end-users?

Notably, CDA Section 230 itself directly refers to the protection of communications by the First Amendment. It expressly legitimizes restrictions by a broad category of Internet service providers, including access providers, hosting providers and search engines, on obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable material, *whether or not such material is constitutionally protected*. In other words, the implications of the First Amendment in this context is exclusively vertical.[428]

Furthermore, the provision has had another effect on First Amendment doctrine and case law. If it applies, there is no need for consideration of the First Amendment for the liability standard for third party communications, since the protection is absolute. In other words, it often blocks the First Amendment from coming into play. This means that the First Amendment, which has had a tremendous impact on United States defamation and tort law, has been of small direct value in some of the most important legal decisions about the legal governance of defamatory information flows on the Internet.

[425] There is limited case law about the scope of CDA, Section (c)(2). See e.g. *Zango, Inc. v. Kaspersky Lab*, Inc., 2009 WL 1796746 (9th Cir. June 25, 2009).

[426] See Tushnet 2008.

[427] For empirical data on the application of CDA, Section 230, see Ardia 2010.

[428] Arguably, the Congressional Findings in 47 U.S.C. § 230 (a)(1-5) could be seen to incorporate free speech values, for instance: "*(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse[...]*". The Congressional Policy statements in 47 U.S.C. § 230 (b), however, do not contain statements that could be interpreted as a reference to the promotion of free speech values.

If the argument is taken seriously that CDA Section 230 codifies free speech values, as is popularly claimed or assumed,[429] this implies that the First Amendment also sanctions the discretion of on-line intermediaries to decide which communications to carry over their networks and on their platforms, because that is what this provision also does. This is mostly in line with the interpretation of the First Amendment in the United States outlined above, which focuses on the protection of the discretion of the owners of the means of communication in the networked information environment.[430] This could also means that the Federal Communications Commission, which recently started to develop policies to promote Internet freedom, including content and application interconnection for Internet end-users, is fighting an uphill battle. Interestingly, the FCC defends these policies to promote open Internet access and end-to-end connectivity of content and applications in the context of broadband, by referring to generally recognized free speech principles as well as the general policy statements included in CDA, Section 230 (b) (1-5). It seems to take the moderate view that free speech values do not legally require but do allow government regulation to promote them. Remarkably, however, the FCC fails to take into account the wide discretion that is offered to broadband providers in CDA, Section 230 (c)(2), even though it is basing its ancillary authority to impose the open Internet standards on CDA, Section 230, and this authority is contested from the start by large American broadband providers. In 2011, a U.S. Court of Appeals denied the FCC its claimed authority to restrict broadband provider's ability to interfere with communications on its networks. The issue can be expected to be further addressed by American courts in the future.[431]

To conclude this discussion of CDA section 230, a final general observation is in place. It could be argued that the most significant result of this blanket immunity for Internet intermediaries is that it abolished the relevance of the traditional connection between the intermediaries' (editorial) control over third party communications on the one hand and the legal responsibility for these communications on the other hand. In the press and paper age, the notion of editorial control seems to have functioned mostly intuitively. These intuitions did not readily translate to the online context, in which the functional interference with content flows by different types of entities was taking a different form, for instance through third party editors or the application of filtering and selection software.

More broadly, the functional interference of different players in the networked information environment can relate to access, selection, navigation, creation, aggregation and transport of content in the network. The proper role and responsibility of the various entities that are carrying out these functions is complex, while the public interests are considered to be great. Considering the (initial) lack of understanding by the Courts how to translate these notions to the online context, combined with the willingness to ensure the unhindered developments of a strong Internet industry, it may have been justified to pass the provisions in CDA, section 230. This provision is, however, a rather simplistic answer to the fundamental questions about the way in which control and discretion by intermediaries should bring some degree of responsibility, as well as reflect implications for the protection of these intermediaries under the First Amendment. It has, until now, blocked more nuanced legal developments

[429] See e.g. Stone 2010.
[430] See Section 6.3.3.
[431] See Speta 2010.

in this field. In addition, it may have strengthened the view that the First Amendment stands in the way of - instead of pointing towards the need for - equal access regulation in the context of Internet access providers to safeguard the effective exercise of the right to freedom of expression in the networked information environment.

6.4.5 EU Directive on Electronic Commerce and freedom of expression

In Europe, the Ministerial Bonn Declaration from 1997, which predates the ECD, was one of the first official texts to address the relation between intermediary liability standards and the principle of freedom of expression. The Bonn Declaration asserts that the rules on responsibility "*should give effect to the principle of freedom of speech, respect public and private interests and not impose disproportionate burdens on actors*".[432] The ECD, in turn, refers to the right to freedom of expression in the context of the freedoms of the European Internal Market, namely the free movement of goods, services and the freedom of establishment. It guarantees these economic internal market freedoms, amongst other things, by introducing the country of origin principle for Information society services.

Recital 9 ECD ties the free movement of information society services to the right to freedom of expression as enshrined in Article 10 ECHR. Compared to the DMCA, the safe harbors in the Directive are not very precise and do not reflect the principle of due process if material is taken down after a notice. The lack of precision is left to the Member States and self-regulatory codes of conduct, to be discussed further below. Recital 46 ECD does provide that "*the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level.*"[433] This recital reflects the view that freedom of expression imposes some restrictions on ISPs in view of the expressive interests of users of their network and communications services.

The precise relation between the right to freedom of expression and the safe harbors depends on the law of the Member States. In general, it is important to note that the ECD *harmonizes* aspects of the internal market for information society services. As always, such harmonization efforts have to respect the European Union's constitutional principles of proportionality and subsidiarity. Notably, the harmonization of the liability of intermediary activities relating to the Internet was not complete. The ECD mirrors the safe harbors in the DMCA adopted 2 years earlier, but did not address the liability for linking and information location tools. This will be discussed in more depth in Chapter 9. Notwithstanding the room for different choices with regard to the implementation of the safe harbors, most Member States have implemented Article 12-15 ECD quite literally. In particular no member state has introduced additional legal safeguards in line with Recital 46 to respect freedom of expression, for instance by codifying a notice and takedown process and a put back option. Typically, self-regulatory codes of conduct that address ISP notice and takedown practices, such as the latest notice and takedown code of conduct in the Netherlands, do not contain a reference to the right to freedom of

[432] See European Union Ministers 1997.
[433] Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC).

expression, assuming the unproblematic status of these types of private self-governance under constitutional guarantees .[434]

6.4.6 Self-regulatory paradigm for ISPs in the EU and the right to freedom of expression

As mentioned earlier in this chapter, the primary concern with the self-regulatory paradigm from the perspective of freedom of expression is that it turns ISPs into the (private) censors of the Internet. This concern seems to be understood in the European context.[435] Its consistent implementation into existing regulation and policy, however, is less successful.[436]

Generally speaking, the notion of self-regulation stands for to the regulatory practice in which private entities are entrusted with some of the elements of regulation, in particular norm formation, adjudication, and enforcement.[437] It is usually contrasted with command and control types of regulation, in which the law seeks to directly define and enforce the legal boundaries of lawful acts in a certain sector of the industry.[438] The related notion of 'co-regulation' or what is also called 'regulated self-regulation' refers to the involvement of the state in self-regulatory frameworks.[439] Co-regulation is the more appropriate term for regulatory activity in which the state is not absent but establishes the basis for self-regulation in the law, for instance in its general media and communication policies. The term co-regulation is usually restricted to self-regulation in which there is a legally formalized role of public authorities.

From the perspective of the right to freedom of expression, an important question with regard to the choice for self-regulation is whether an informal, but still active, government role aimed at the restriction and removal of certain content or communications on the network is consistent with the demands of Article 10 ECHR. Interferences with the right to freedom of expression by public authorities must be prescribed by law. This means, first of all, that interferences must have a legal basis. Second, it means that interferences must fulfill the quality of law standards: they must be foreseeable and accessible. In other words, the framework of Article 10 ECHR attaches value to the way in which interferences by public authorities are legally grounded and delineated. An act by public authorities that constitutes an interference, but is without legal basis, would not survive the test of Article 10.

At the same time, it is clear that an informal role of public authorities in self-regulatory frameworks makes it harder to argue that actual interferences with the free exercise of the right to freedom of expression that result from the application of this framework in practice should be attributed to these public authorities. If the framework is, legally speaking, voluntary, the responsibility for restrictions on information flows lies primarily with private actors. Moreover, this state of affairs is in many ways consistent with the implications of the right to freedom of expression in vertical relations. However, it

[434] See Van Hoboken 2008b.

[435] See e.g. Hans-Bredow Institut 2006, pp. 149-152. Tambini et al 2008. For the U.S. context, see Bambauer 2011 forthcoming.

[436] For a critical overview of the threat of the self-regulatory paradigm for the right to freedom of expression, see European Digital Rights 2011.

[437] See Price & Verhulst 2005, pp. 3-4. For a detailed discussion, see Hans-Bredow Institut 2006.

[438] On regulation more generally, see Baldwin & Cave 1999.

[439] See generally Hans-Bredow Institut 2006. See also Tambini et al 2008.

also points to the need to keep in mind that the characterization and structuring of restrictive state action as self-regulation, could be used to obscure the public authorities' role and circumvent the applicable constitutional safeguards. Safeguards that would apply more clearly in case of a formalized role.[440] ISP codes of conduct with regard to illegal, infringing and harmful third party content and communications are often drafted at the initiative and under supervision of public bodies, and heavily influenced in their content by government officials. Moreover, in what is sometimes called the raised eyebrow tactics, public authorities or the legislature sometimes gives a (last) chance to the industry to fix 'the problems' themselves. More generally, industry codes of conduct are typically drafted not in the absence of the law but within the existing legal boundaries, which already serve to incentivize certain types of private governance in view of public policy objectives. And whereas in the case of press governance, there is no extensive regulation of the 'services' provided to the public, in the case of access providers, the existence of detailed sector-specific regulation implies that the regulatory relation between industry and the state is much more intense from the start.

So, to what extent, and in what ways have these considerations with regard to implications of the right to freedom of expression for self-regulation played a role in the EU regulatory and legislative context? The establishment of the self-regulatory paradigm for online media and information services can be traced back to the 1998 Council Recommendation on the protection of minors and human dignity, which carried the full title: "*on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity*".[441] The earlier European Commission green paper on the protection of minors and the communication on illegal and harmful material online, which resulted in this Council Recommendation, contained many explicit references - as well as a detailed overview in the annex - of the demands of Article 10 ECHR in the context of content regulation for media and information services, even though it remains rather vague on the implications for self-regulatory frameworks in particular.[442] The 1998 Council Recommendation, however, mainly refers to the general principle of freedom of expression. The included 'indicative guidelines for the implementation of the self-regulation framework', state "*that the proportionality of the rules drawn up should be assessed in the light of: the principles of freedom of expression*" and other fundamental interests.[443] However, the way in which this complex undertaking should take place is left to the stakeholder process at the national level. The recommendation does not introduce or mention any specific restrictions on the self-regulatory codes of conduct which could be seen to follow from the right (and principle) to freedom of expression. In particular, it does not address the question about the possible restrictions following from Article 10 ECHR for the proper role of public authorities in self-and co-regulatory frameworks.

[440] On the impermissibility of this under the Convention, see ECtHR 25 March 1993, *Costello-Roberts v. United Kingdom.* See also Hans-Bredow 2006, p. 152.
[441] Council Recommendation 98/560, 1998 O.J. (L 270), 48 (EC).
[442] See European Commission 1996c.
[443] Council Recommendation 98/560, 1998 O.J. (L 270), 48 (EC).

The lack of stipulation of freedom of expression implications for the role of the state in self-regulation of information flows in light of traditional public policy perspectives is somewhat perplexing. From the perspective of the right to freedom of expression and the general obligation on the state to ensure the effective exercise of the rights and freedoms under the Convention, it is clear that the state should not contribute or promote a self-regulatory framework which results in extensive private censoring of legitimate information flows online. It would also be inconsistent with the state's obligations under the right to freedom of expression to deliberately incentivize private parties to do what it would not be allowed to do itself.

In the following section, one of the most controversial self-regulatory developments in the context of Internet access providers will be discussed in more detail, namely the filtering and blocking of parts of the Internet or communications on the network by Internet access providers. The topic of Internet filtering Internet access providers is chosen for a number of reasons. First, it has raised an intense debate about the proper role of government with regard to Internet regulation and the right to freedom of expression. Second, it relates to the basic questions about the proper boundaries of access regulation in the ISP context. Third, it is not only generally accepted that freedom of expression should be taken into consideration in these contexts, but also official legal documents contain strong references to the right to freedom of expression. Fourth, the legal and legislative debate about filtering by Internet access providers is relatively mature. There is even a case before the European Court of Justice about the filtering of communications by access providers. And finally, Internet content filters in many ways perform a similar function as search engines. Together they could be seen to fall into the broader category of selection intermediaries. The discussion will be mostly restricted to the European context.

6.5 Internet filtering by access providers

6.5.1 Background

The development and application of Internet content filters (hereinafter: 'Internet filters') is a central issue in the regulatory debates about freedom of expression on the Internet and the role of ISPs in providing access to content.[444] There are many types of Internet filters and they are deployed in a variety of circumstances. This section will address the type of Internet filter that limits the accessibility of material on the Internet for end-users and discuss one case relating to the possible filtering by access providers of copyright infringing communications between end-users. The application of filters by hosting providers or online service providers such as YouTube will not be discussed as well as questions relating to the technical aspects of Internet filters.

Internet filters can raise issues under the right to freedom of expression, but generally filtering technology can perform legitimate functions. They are important from the perspective of the broader function of the selection of content in the public networked information environment and thereby fall in

[444] See e.g. Sieber & Nolde 2008; McIntyre & Scott 2008; Tambini et al 2008; Dommering 2009; Dommering & Asscher 2006; Heise Online 2009; Heins et al 2006; Deibert et al 2007; CoE, Committee of Ministers, Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters, 2008.

the broader category of what could be called selection intermediaries.[445] Selection intermediaries govern the accessibility, i.e. relative reachability of material on the Internet. Examples of selection intermediaries include Internet filters, search engines, recommendation services, and Internet Service Providers ('ISPs') that block or filter content on the basis of their contents.[446] Selection intermediaries fulfill an important function in our information environment, which is characterized by abundance. They help end-users to find and select the information they consider relevant or useful, and can exclude information that they are not willing or allowed to access, for instance because it is harmful or illegal.

Internet filters are quite commonly used and installed by end-users, for instance by parents to prevent access to content by their children. They are also widely deployed by private actors on their networks, for instance by employers or Internet cafes. They can be installed in the public sector to restrict access to content or applications.[447] In public institutions such as schools and libraries, which fulfill a particular function or serve an audience that may warrant stronger selection of the accessibility of information, the application of Internet filters is quite common.[448]

Internet access provider can use, be asked to use, or legally ordered their intermediary position to establish gatekeeper control over information flows on the Internet by using Internet filters. The typical context of these measures would be the prevention of access to illegal material on the basis of lists of such material kept and maintained in the context of enforcement of child pornography legislation by criminal law enforcement agencies and special private or private-public entities.[449] In Europe and the United States, the issue of child pornography, has led to a range of regulatory and self-regulatory activity, to use blacklisting of web destinations. In Europe, such blacklisting was first introduced in the United Kingdom and Norway. A European Commission proposal for a new Directive includes an explicit reference to this kind of framework. In a number of countries in and outside of Europe, ISPs have agreed with public authorities to filter child pornography at the network level, for instance in the U.K.. In some jurisdictions public authorities require access providers by law to use filtering products at the network level.[450] Proposals for similar legislation or regulatory practices have been discussed in Germany and the Netherlands. At the level of the EU, there have been ongoing discussions about a Directive that would establish the EU regulatory framework for the filtering of child pornography at the European level.

6.5.2 Internet filters and the right to freedom of expression

The application of Internet filters raises a number of concerns under the right to freedom of expression. The first concern is related to the interests of end-users under the right to freedom of expression, and can be expressed most aptly in terms of end-user autonomy. If Internet filters are deployed, without the

[445] See Section 3.2.2.

[446] See Van Hoboken 2009.

[447] In the United States, some of the government funding to public libraries has been made conditional on the installation of such filtering software. *See U.S. v. American Library Association*, 539 U.S.194 (2003).

[448] For a discussion on Internet filters and libraries, see Section 7.4.5. Schools often restrict access to information online with Internet filters.

[449] See e.g. Schafer 2010, pp. 535-538. For a discussion of the technical aspects of the UK Cleanfeed system and the possibility to reverse engineer the list of blocked illegal content, see Clayton 2006.

[450] For a comprehensive overview and discussion of global Internet filtering see Deibert et al 2007.

end-user's consent, knowledge or control over the filtering of content, the end-user is prevented from accessing information freely. In addition, the deployment of certain filtering products by access providers, for instance those that are aimed at blocking the distribution of unauthorized copies of copyright protected works, would imply that all communications would be screened and monitored with the use of deep packet inspection (dpi) technology. A second concern is related to the interests of online information and service providers, and information sources more generally, to reach an audience. A third concern, which directly impacts on the weight of the first two concerns is related to the actual functioning and imperfection of Internet filters in relation to the goals for which they are often being promoted.

Although Internet filters are quite imperfect and ineffective to prevent access to content, they are still widely promoted as a solution for suppressing access to or the communication of illegal or infringing material.[451] In light of the guarantees relating to freedom of communication, it is questionable whether the current Internet filtering products could be an acceptable solution.[452] It is well known that Internet filters applied by access providers based on DNS filtering can be easily circumvented and the same is true for more advanced types of filtering at the network level. In fact, Western democracies, the United States in particular, are actively promoting the development of effective filtering and blocking circumvention software to support political dissidents and activism in Countries like China and Iran.[453] Moreover, the imperfection of blocking and Internet filters in terms of their effect on legitimate content has always posed significant restrictions on the possibility of requiring filtering by access providers. Existing products are notoriously inaccurate, often preventing access to sites that should not be blocked while failing to block many that should.

The capabilities of different kinds of Internet filters that access providers could deploy on their network plays a role in the discussion about the proper responsibility of Internet access providers for facilitating access to illegal content and infringing communications. Under general principles of law, one cannot be required to do the impossible.[454] However, the safe harbor legislation in the E-Commerce Directive anticipated increased technological efficacy. Recital 40 of the E-Commerce directive provides that:"

> […] the provisions […] relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.[455]

Hence, the development of increasingly sophisticated network management and filtering technologies for access providers could make filtering obligations on Internet access providers appropriate in the view of the EU legislature. Article 21 (2) of the E-Commerce Directive instructs the European Commission to

[451] See European Commission 2009.
[452] Stol et al 2008.
[453] See Figliola et al 2010.
[454] See e.g. Koelman 2000.
[455] Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC).

"*analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments*", in its evaluations of the Directive.[456]

Fundamentally, however, the issues raised by the imperfection of Internet filters may not be a technological one. Internet filters are inherently imperfect, at least if one takes content and copyright related legal restrictions on the freedom to communicate seriously. Automated filters will always filter too little and too much at the same time. The reason is that they try to build complicated context dependent norms about the lawfulness of communications into technology. Of course, it is possible that these imperfections would be accepted by the law, but this would simply cause the distinction between lawful and unlawful communications to change from a legal distinction, ultimately requiring a judgment by a court, to a distinction governed by technology.[457]

The mandatory application of Internet filters ordered by public authorities is also considered problematic because they can be seen as prior restraints with regard to the source of the blocked material.[458] As we discussed in the chapter 5, both Article 10 ECHR and the First Amendment contain a heavy presumption against the permissibility of prior restraints. And as mentioned above, the possibility to circumvent the filters implies that the material itself remains accessible, at least for more savvy end-users. For illegal material, such as child pornography, the fact that the material itself remains online, whereas public authorities should pursue those responsible for the publication and the abuse has been one of the strongest arguments against filtering. Clearly, these circumstances also make the prior restraint all the more problematic.

Because of these problems relating to mandatory Internet filtering from the perspective of freedom of expression, the application of Internet filters has mostly been left to the market and policy has focused on stimulating the market for Internet filtering products, thereby ensuring that end-users have effective means to prevent access to content, for themselves and their children in particular. CDA Section 230 can be argued to have this aim and allows for the use of Internet filters by access providers and other intermediaries. It did not imply that ISPs ought not to restrict access to material online, but granted ISPs discretionary power needed to deploy filtering technology voluntarily without risking liability. [459] In the European context, the situation is different, since the safe harbor for Internet access providers in Article 12 ECD does not contain a provision that protects them against third party claims if they would be actively interfering with traffic on their networks. In fact, in the European context, by installing Internet filters aiming to restrict access to child pornography or other online destinations, access providers may run the risk of increased liability and injunctions, since other interested parties may have lists of websites that should be filtered also.[460]

[456] The first report did not address this possibility, which may be explained by the fact that it mostly focused on whether the Directive was implemented (properly) in the Member States. See European Commission 2003.

[457] For a general discussion of the desirability of 'codifying' regulation into software see Dommering & Asscher 2006. See also Grimmelmann 2005; Lessig 1999; Reidenberg 1998.

[458] See Dommering 2009.

[459] See European Commission 1996b, p. 14.

[460] This is the subject of ongoing legal debate and litigation across Europe.

In 2008, the Committee of Ministers of the Council of Europe issued as recommendation on freedom of expression and Internet filters, which addresses some of the concerns regarding Internet content filters from the perspective of Article 10 ECHR.[461] The recommendation and the underlying report acknowledge both the legitimate function of Internet filters and the ways in which Internet filters can impact on freedom of expression and information. It explicitly addresses some of the perceived requirements of Article 10 ECHR in this context,[462] and addresses the fundamental interests of information providers and end-users. The recommendation calls upon the Member States of the CoE to take measures with regard to Internet filters in line with a set of guidelines promoting user notification, user awareness, and user control of Internet filters and accountability of the private and public parties involved. The recommendation makes a difference between mandatory filtering and the use of Internet filters by public entities, such as public libraries and schools on the one hand, and their use by private entities, such as enterprises in the context of Internet access in the workplace on the other hand and addresses the implications of freedom of expression for both situations.

6.5.3 Mandatory filtering and the interests of information providers

Internet content filtering, in the form of blacklisting by access providers, deprives the information providers that are being filtered from being received by significant parts of the population. To what extent are these interests of information providers protected under Article 10 ECHR?

If the filtering is mandatory, the access provider could assert the protection of Article 10 ECHR. This protection is partly informed by the interests of speakers to reach an audience.[463] First of all, for any source to be blocked which would not be judged illegal by a proper authority, it could contest the validity of blocking it for its end-users. It would also be able to argue that mandatory filtering would cause it to sometimes block legitimate information sources which would be accessible otherwise. It is possible that the access provider does not protest against mandatory filtering. In these cases, (lawful) information providers that would be blocked could assert their right to impart information and ideas freely. The information provider itself would also be able to claim that the filtering amounts to an interference with its right to impart information and ideas freely as protected under Article 10 ECHR.

The question is whether this interference would be proportional and how the proportionality test should be applied. The United States Supreme Court has made clear in a number of rulings relating to legislation aimed to protect children from accessing harmful content, that the First Amendment involves strict scrutiny, if it targets the publicity of material at the source and requires the measure to be "*narrowly tailored to serve a compelling Government interest, the least restrictive means available for the Government to serve the interest of preventing minors from using the Internet to gain access to*

[461] CoE, Committee of Ministers, Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters, 2008. See also CoE, Report of the Group of Specialists on human rights in the information society (MC-S-IS) on the use and impact of technical filtering measures for various types of content in the online environment, CM(2008)37 add, 26 February 2008.

[462] The recommendation of the CoE's Committee of Ministers are not binding.

[463] See Section 6.3. See also Section 5.5.

materials that are harmful to them."[464] The alternative, considered by the Court, was the availability of filtering software, which could be installed and controlled by end-users themselves.

The Council of Europe recommendation qualifies the use of Internet filters in the public sector as an interference with the right to freedom of expression and makes the test of article 10 second paragraph more explicit. It demands that filtering of Internet content in electronic communications networks operated by public actors or mandatory filtering at the ISP level has to concern "*specific and clearly identifiable content*", "*a competent national authority should have taken a decision on its illegality*" and "*there should be an opportunity to have this decision 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*".[465] Furthermore, the guidelines stipulate that Member States have to ensure that there is an evaluation of the proportionality of filters before and during their implementation in terms of their possible effects on the unreasonable blocking of content. As regards the interests of information providers, the Recommendation states that Member States "*should [...] 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.*" This last obligation is also applicable to the use and application of filters in the private sector.

6.5.4 Voluntary filtering by access providers and the interests of information providers

The situation changes if the filtering by access providers is voluntary. In these cases, there remains a de facto horizontal conflict between the ISP that imposes filtering and the information providers it is blocking. The legislative resolution for these conflict of interests in the United States is laid down in CDA, Section 230(c)(2), which was discussed in Section 6.4. This provision grants access providers and other intermediaries wide discretion to decide to block – in good faith - indecent or otherwise objectionable content, even if it is constitutionally protected.

In the European context, this horizontal conflict would lead to a balancing of interests of information providers under Article 10 ECHR (leaving aside possible other interests unrelated to the right to freedom of expression such as economic freedom and unfair competition) with the right to the free exercise of private property of the ISP. Typically, there will be a wide margin of appreciation with regard to the way in which a positive obligation on the State to guarantee the effective exercise of the right to freedom of expression in horizontal relations, if it exists, will have be fulfilled. Normally, the protection of the interests of information providers in the context of filtering access providers to use filtering will have to be considered to lie in the realm of discretion of the state. National law may place more stringent

[464] *ACLU v. Mukasey*, cert. denied (Sup Ct. Jan 21, 2009), *ACLU v. Mukasey*, No. 07-2539 (3d Cir. July 22, 2008); *Ashcroft v. ACLU*, 542 U.S. 656 (2004), 322 F.3d 240 (2003); *Ashcroft v. ACLU*, 535 U.S. 564 (2002), , 217 F.3d 162 (Third Circuit 2000); *ACLU v. Reno* 31 F. Supp. 2d 473 (ED Pa. 1999).

[465] Article 6 ECHR, first paragraph: "*In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgement shall be pronounced publicly by the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.*"

obligations on the state to protect information providers from being blocked by access providers.[466] Mandatory positive obligations would only arise when individuals would be prevented to effectively exercise their freedom of expression or when pluralism of the information environment would be clearly at stake. In cases in which blocking by access providers would lead to a situation that would deprive a legitimate online speaker from reaching an audience completely, the best argument for a strict positive obligation on the state could be made.[467] Pluralism could be argued to be endangered when over-blocking by Internet filters shows structural biases with regard to certain types or sources of speech or certain types of issues.

Arguably, the interests of information providers can be easily safeguarded by introducing certain levels of transparency and accountability into the filtering regimes. With that in mind, the Council of Europe Recommendation calls on the Member States to safeguard the interests of Internet content providers, by providing for effective and readily accessible means of recourse and remedy, including suspension of filters, in cases where content has been blocked unreasonably.[468]

A final question is whether the law could and or should require Internet access providers not to filter at all. In general, this is probably not the case. It is generally accepted that there are good reasons for Internet access providers to interfere with communications on their networks, for instance in the context of unsolicited communications. As regards content, there seems a growing consensus that it is important to keep the Internet as a platform to reach audiences and consumers open for everyone. Access providers have not yet started to block content on a wider scale than the child pornography context, although it must be noted that also in this context there are many examples of websites, the blocking of which, raises serious questions.[469]

6.5.5 Internet filters and the interests of end-users

Internet filters could implicate the interests of end-users, in particular if they are deployed outside of their control. In these cases, Internet filters would interfere with the freedom of end-users to receive information and ideas, in other words the end-user's autonomy. If Internet filters are deployed by end-users, for instance to prevent their children from accessing certain types of material, and end-users have control over what is being filters, most of the concerns over freedom of expression disappear.[470] One hypothetical conflict remains, namely between a speaker that wants to reach an end-user which decides

[466] Which is not the case in for instance The Netherlands. See HR 12 maart 2004, *XS4all v. Ab.Fab* (Rejecting the Amsterdam Court of Appeal's argument that Internet access provider XS4all had to permit restrictions on its free exercise of its property rights in its computer and transmission capacity, because of the nature of the services it was offering and in particular the public interests involved in its services, and arguing that Article 10 ECHR, in principle, could not be invoked in defense of an infringement of someone's (free exercise of its) property rights. XS4all sought an injunction to prevent Ab.Fab from sending unsolicited advertising to its customers.)

[467] See discussion of *Appleby* in Section 6.3.1.

[468] CoE, Committee of Ministers, Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters, 2008.

[469] For an overview of controversially blocked sites in the U.K., see Clayton 2009.

[470] For instance, if a child would be prevented from accessing the Internet in its parent's home at all, the law would not interfere with this governance of the private sphere. See generally Benkler 2001.

to block that particular source. In such cases, the protected interests of the end-user carry more weight, for at least two reasons. First, Internet access involves a computer terminal that simply allows for the ability to select what information to access and what to block. This freedom is not only protected under Article 10 CEHR, but the way it is exercised is typically part of the private sphere as well.[471] Second, in this private sphere, the end-user cannot be forced or even expected to listen.[472]

Of course, end-users, when deploying filters, might have control in practice, but in reality the Internet filters are created and maintained by others. Internet filtering products aimed to promote child safety are often opaque – the blocking lists can for instance be protected as trade secrets - and have limited options of redress. And the deployment of Internet content filters often does not fully respect end-user autonomy. In fact, Internet filters are typically promoted by public authorities as a solution for problems that are the result of the freedom of end-users, namely the *possibility* to access illegal information. The filtering of content by ISPs does not respect end-user autonomy by definition, since this would give the choice to access the material to the user. Hence, there remains room for public policy to enhance end-user autonomy in the context of Internet filters. It is logical for such public policy to be aimed at end-user autonomy with regard to lawful and legal material.

The respect for end-user autonomy seems to have been the dominant concern underlying the CoE Recommendation on Internet filters and freedom of expression.[473] First of all, the guidelines provide that end-users, where appropriate, must be able to control the level of filtering. The guidelines further stipulate that end-users should have the possibility to challenge the blocking or filtering of content and to seek clarifications and remedies. With respect to the end-user's ability, where appropriate,[474] to activate and deactivate filters and to be assisted in varying the level of filtering in operation, the guidelines call upon the Member States to ensure, in cooperation with the private sector and civil society, the existence of a number of more detailed guarantees. It is provided that end-users should receive guidance regarding the manual overriding of an activated filter, more specifically 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). Furthermore the recommendation states that content that is filtered by mistake or because of an error has to be accessible without undue difficulty and within a reasonable time. With regard to the use and application of Internet filters by the public sector, Member States have to 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.

Of course, Internet end-users cannot simply be placed at the receiving end of the communicative process. In the networked information environment, the end-user are also the source of illegal and infringing communications or material. Peer-to-peer distribution technology has harnessed the potential

[471] See e.g. in the United States, *Stanley v. Georgia,* 394 U.S. 557 (1969).

[472] See Section 5.5.1.

[473] CoE, Committee of Ministers, Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters, 2008.

[474] The recommendation does not clarify when this would be appropriate.

of the Internet for end-users to distribute content between end-users. The sharing of copyright protected material, such as music, films and software, with the use of such peer-to-peer technology has led to a discussion about the imposition of filtering obligations on ISPs to filter out infringing communications.[475]

In Belgium, the rights holders organization SABAM has legally pursued this option most aggressively. It sued Internet access provider Tiscali in 2004 for injunctive relief. It asked to Belgium Court to order Tiscali to stop the infringing communications on its network. The Court of first instance ordered the Internet provider "*to mak[e] impossible any form of sending or receipt by its clients, by means of 'peer to peer' software, of electronic files containing musical works that are part of the SABAM repertoire*."[476] Tiscali appealed the Court's judgment, and the Belgium Court of Appeals has referred questions about the permissibility of the injunction under European law and the fundamental rights to freedom of expression and private life to the European Court of Justice. More specifically, the Court has to address the question, whether an injunction on access providers that obligates them to identify and block all copyright infringing communications by its subscribers is permissible under Article 12 and 15 of the E-Commerce Directive and the right to freedom of expression.[477]

The ECJ still has to hand down its judgment, which will be of great significance for the question about the limitations on the possibility to require filtering by access providers that follow from the right to freedom of expression of end-users. If the Court follows that Advocate General's opinion, these limitations would stand in the way of the kind of filtering as was sought by rights holders in this context. The Advocate-General clarifies that what is presented as a simple injunction in civil proceedings would in effect amount to the permanent imposition of systematic and universal filtering of all the communications on the network, which would eventually have to be extended to all ISPs in the future to be effective.[478] This general and far-reaching character of the sought measure leads the Advocate General to the conclusion that a specific legal basis would be needed to impose such a system, which was lacking in Belgium Law. In the Advocate's General view, the measure would apparently be disproportionate, both from the perspective of the rights and interests of the access provider, as well as its end-users.[479]

6.5 Conclusion

In contrast with the regulatory model for the press, traditionally, there has always been extensive regulation of communications network providers. However, content regulation tends to be either absent or minimal and raises issues under the right to freedom of expression. In vertical relations, the owners of the means of communications such as Internet access providers can assert their own right to 'freedom of expression' against government interference, and this right includes the right to access,

[475] For an overview of filtering by IPSs in light of copyright infringements, see Angelopoulos 2009.

[476] District Court of Brussels, 29 June 2007, No. 04/8975/A, *SABAM v. Tiscali (Scarlet)*, published in CAELJ Translation Series #001, 25 Cardozo Arts & Entertainment Law Journal, 2008.

[477] ECJ, Reference from the Cour d'appel de Bruxelles, 5 February 2010, *Scarlet v. SABAM*, Case C-70/10.

[478] ECJ, Conclusions of Advocate General M. Pedro Cruz Villalón, 14 April 2011, *Scarlet v. SABAM*, Case C-70/10, par. 66.

[479] Id., § 67,68, 87, 113.

receive and transmit. Even more than in the case of the press, these rights are informed by the communicative interests of the users of such communications networks. These interests in communicating freely with the use of steadily improving communications techniques (postal mail, telegraphy, telephony and the Internet) were clearly served by a practice in which the network owners would not restrict communications over the network. In that respect, the regulatory concepts of 'common carrier' and 'universal service' which have helped to shape the regulatory models for communications network providers, can also be seen as informed by the right to freedom of expression users of the communications network. Universal service requirements acknowledge the way in which access to communications networks is essential to societal participation. The common carrier requirement guarantees equal treatment of users of the networks, thereby limiting the discretion of network providers to restrict information flows.

Convergence of media and communications has complicated the regulatory environment for communications providers significantly. Internet users, can use one and the same Internet connection, to correspond privately, watch 'television' or broadcast their views for a global audience. The facilitating role of Internet access providers with regard to the *public* networked information environment means that the normative role of the right to freedom of expression for the governance of communications networks has increased in importance. Traditionally, the constitutional right to privacy and confidentiality of private correspondence, such as protected by Article 8 ECHR, were of relatively greater importance.

In this Chapter, the way in which Internet access providers have been involved in content regulation in the networked information environment was used to study the implications of the right to freedom of expression in this context. This regulatory framework was shown to consist of safe harbors setting the legal boundaries for the liability of ISPs for third party communications on the one hand, in combination with an emphasis on further self-regulatory or co-regulatory action on the other hand. The case law relating to these laws as well as their legislative history show that freedom of expression has been taken into account in this framework but it remains strongly debated to what extent this has been done properly.

When thought through, legal obligations on access providers to prevent the use of their communications networks for illegal purposes, or the possibility to access illegal material, lead to clear problems under the right to freedom of expression, in particular the conditions set out in Article 10 second paragraph and possibly Article 8, second paragraph. Such general obligations could only be adhered to with the application of Internet filters, the mandatory application of which is more than constitutionality doubtful. Although the pressure to move towards stricter legal responsibility of Internet access providers remains and proposals to require blacklisting by access providers are debated in European Parliament and elsewhere, the right to freedom of expression has been one of the reasons these government interferences with the right to freedom of communication have mostly not materialized into actual laws.

While there are hardly any legal obligations on access providers to interfere with the communications on their network, the self-regulatory paradigm has informed public authorities to seek voluntary

cooperation of access providers to regulate content nonetheless. For the most part, public policy aimed to restrict the accessibility of content by access providers has not led to command and control types of regulation but has sought to minimize the official role of the state while at the same time still aiming to achieve more restrictive practices by ISPs. This may partly be the case, as in the case of the governance of the press, precisely because of the right to freedom of expression. However, the relation between access providers and Internet users is quite a different one compared to the press, looking at the press as an intermediary in the public communicative process. Whereas for the press the selection of information and ideas for publication is sanctioned by the right to freedom of expression *because* of the importance of editorial freedom and the fact that this is what the press is supposed to be doing all along, the exclusion or blocking of communications by access providers is hard to harmonize with the ideals underlying freedom of expression, in particular when taking stock of the impact this would have on lawful communications over the network.

This leads to the most complicated issue touched upon in this chapter: how should the impact of the current legal framework on the horizontal relations between access providers and Internet users be evaluated from the perspective of the right to freedom of expression. Or to put it differently, what are the proper implications of the right to freedom of expression for the legal discretion of access providers to restrict communication over their networks? Two different general points of view on this debate emerged in the analysis.

The first, which we may best call the user freedom theory, tends to equate the right to freedom of expression in these potential conflicts of interests between access providers and users to the communicative interests of Internet users. In this theory, if freedom of expression legally requires anything with regard to the legal governance of horizontal relations between access providers and end-users, it would be that government would have to protect the user's interest against undue interferences by Internet access providers, for instance through the establishment of new types of common carrier and universal service rules and through the establishment of due process guarantees in case of specific legitimate interferences with the flow of content or use of the network. In other words, the role of the law should be aimed at the realization of the free exercise of the right to freedom of expression by Internet users. The various Council of Europe recommendations touching upon these issues testify of the dominant nature of this perspective in European freedom of expression doctrine. Within the boundaries of this theory, much debate remains about the nature of the implications of the right to freedom of expression in this context, in particular whether there is a real obligation for the state to act or if it is better to speak of freedom of expression in this context as a regulatory principle.

The second perspective, for which support - and opposition, to be clear - can be found in the United States, tends to equate the right to freedom of expression with the discretion over the use over communicative means as established by the free market. This theory may be best called the ownership discretion theory of freedom of expression. From this perspective, the right to freedom of expression protects the owners of the means of communications (and media more generally) against legal interferences with the freedom to decide how to use those means in the free market. The result of this theory is that the possibility of the government to regulate the horizontal relations between Internet access providers and Internet users to safeguard the communicative interests of the users of the

network is actually restricted by the right to freedom of expression of Internet access providers, more specifically a right not to transmit or to exclude.

From a European perspective, it could be concluded that Article 10 ECHR would most probably not support a claim of the network owners not to transmit, but that any such claim would have to be based on the right to private property. In the United States, the legal mainstream may actually be moving in the direction of allowing a similar claim of Internet access providers not to transmit under the First Amendment. This could have significant implications for the political and legal feasibility of network neutrality regulation.

In the safe harbor framework for Internet service providers, the right to freedom of expression could also be shown to be understood by the legislature as relating to the communicative interests of Internet users. Notably, the way in which freedom of expression has been internalized into the EU intermediary liability regime leaves much room for criticism. No due process guarantees have been prescribed, such as one can find in the U.S. Digital Millennium Copyright Act, the room for injunctions is left wide open, and the hosting safe harbor, the scope of which may be less clear than ever, may incentivize intermediaries to restrict lawful communications. In addition, the role of public authorities in the design of self-regulation has been questionable.

The specific analysis of the internalization of the right to freedom of expression in the United States legal safe harbor framework showed a mixed picture. Some elements in the regulatory framework seem to sanction the discretion of ISPs to disregard the interests of information providers and end-users in horizontal relations. Section 230 of the Communications Decency Act (which is also applicable to search engines) is possibly most striking in this regard. It not only shields against liability, it also provides far-reaching discretion for interactive computer services with regard to third party communications. By studying the background of this provision, which was enacted in 1996, it was further shown how this provision has in many ways prevented freedom of expression doctrine from having a further impact on the proper legal regime for various kinds of Internet service providers in the United States, including search engines. The different legal standards for carrier, distributor and publisher liability as they applied in defamation cases before the Internet, and the way in which editorial freedom and control had played a role in the formation of these standards in a rich set of court decisions have been replaced by a double-edged sword for Internet intermediaries: a shield against liability and legal discretion to block various kinds of content, including constitutionally protected communications.

The two theories mentioned above reflect perspectives on the right to freedom of expression with implications that go well beyond the context of Internet access providers or search engines for that matter. For some, the application of the ownership discretion theory of freedom of expression to the context of the press may be less strikingly absurd than to the context of Internet access providers. In the networked communications environment, however, control over communications with the use of various technologies of control has provided the means for traditionally passive conduits to be more actively involved in the selection and prioritization of content flows on the network, whereas it may have provided others, that tended to be more active with the means to be more passive. Chapter 6 shed some light on the fundamental questions this raises about the way in which freedom relates to

discretion and control relates to responsibility, and the way in which those answers could ultimately find their ways into properly informed laws and regulation for various entities in the public networked information environment.