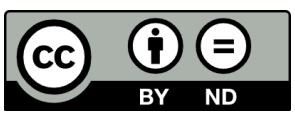
Study of fundamental rights limitations for online enforcement through self-regulation

Institute for Information Law (IViR)
Faculty of Law
University of Amsterdam
www.ivir.nl

Christina Angelopoulos, Annabel Brody, Wouter Hins, Bernt Hugenholtz, Patrick Leerssen, Thomas Margoni, Tarlach McGonagle, Ot van Daalen and Joris van Hoboken

This study was supported by the Open Society Foundations.



Contents

Acknowledgements

This study was supported by the Open Society Foundations.

The authors are listed in alphabetical order.

The authors would like to thank the following persons for their feedback on draft versions of the study: Vera Franz, Joe McNamee, Darian Pavli, João Pedro Quintais, Nico van Eijk and Dirk Voorhoof. They are also grateful to Rade Obradović for research assistance/literature searches.

Thomas Margoni would like to thank the European Union Seventh Framework Program (FP7) for enabling his involvement in this research project.

The research for this study was completed and the websites mentioned were last checked in December 2015.

Executive Summary

The use of self-regulatory or privatized enforcement measures in the online environment can give rise to various legal issues that affect the fundamental rights of internet users. First, privatized enforcement by internet services, without state involvement, can interfere with the effective exercise of fundamental rights by internet users. Such interference may, on occasion, be disproportionate, but there are legal complexities involved in determining the precise circumstances in which this is the case. This is because, for instance, the private entities can themselves claim protection under the fundamental rights framework (e.g. the protection of property and the freedom to conduct business).

Second, the role of public authorities in the development of self-regulation in view of certain public policy objectives can become problematic, but has to be carefully assessed. The fundamental rights framework puts limitations on government regulation that interferes with fundamental rights. Essentially, such limitations involve the (negative) obligation for States not to interfere with fundamental rights. Interferences have to be prescribed by law, pursue a legitimate aim and be necessary in a democratic society. At the same time, however, States are also under the (positive) obligation to take active measures in order to ensure the effective exercise of fundamental rights. In other words, States must do more than simply refrain from interference. These positive obligations are of specific interest in the context of private ordering impact on fundamental rights, but tend to be abstract and hard to operationalize in specific legal constellations.

This study's central research question is: *What legal limitations follow from the fundamental rights framework for self-regulation and privatized enforcement online?*

It examines the circumstances in which State responsibility can be engaged as a result of self-regulation or privatized enforcement online. Part I of the study provides an overview and analysis of the relevant elements in the European and international fundamental rights framework that place limitations on privatized enforcement. Part II gives an assessment of specific instances of self-regulation or other instances of privatized enforcement in light of these elements.

Part II considers the extent to which certain blocking and filtering practices currently used for privatized enforcement online are compatible with fundamental rights, most notably the right to freedom of expression, freedom of information, the right to access information, the right to privacy, data protection rights, the right to a fair trial, the right to an effective legal remedy, freedom to conduct business and freedom to provide services. Three case studies are used for this examination:

1. Non-judicial notice-and-takedown procedures of social networking services;
2. Voluntary use of content-ID tools by hosting providers to avoid liability for illegal content, and
3. Voluntary scanning of private data by online service providers and the subsequent reporting of users to law enforcement agencies.

The case studies take due account of the degrees of (market) dominance and state involvement involved in the examples of privatized enforcement, as well as the availability of remedies.

Drawing on its examination of the European and international human rights framework and the practices and problems revealed by the illustrative case studies, the study explains various ways in which a State may be found to be in breach of its positive obligations for its failure to prevent violations of individuals' fundamental rights as a result of privatized law enforcement by online intermediaries. The study has found that criteria that could prove determinative in this respect include the:

- Existence or development by the State of relevant regulatory frameworks;
- Nature of the interference and its intrusiveness (specific techniques of blocking or filtering could prove determinative) and resultant chilling effect;
- Demonstrable degree of involvement or complicity of the State in the interference;
- Adherence to procedural safeguards by the actor (e.g. transparency, adequacy of information; accessibility of terms, conditions and procedures and foreseeability of their consequences, etc.);
- Availability of independent and impartial (judicial) review and redress;
- Dominant position of actor/availability of viable communicative alternatives;

This study has also sought to fill a normative gap by teasing out the implications of positive state obligations in respect of privatized enforcement measures by online intermediaries. In doing so, it has borne the above criteria in mind, as well as the overarching concern to strike a fair balance between competing rights, and focused on the following positive obligations to:

- Guarantee (media) pluralism;
- Create a favourable environment for participation by everyone in public debate;
- Create a favourable environment for freedom of expression for everyone without fear;
- Ensure effective procedural safeguards and effective remedies in respect of the right to freedom of expression;
- Ensure effective procedural safeguards and effective remedies in respect of the rights to privacy and data protection;
- Guarantee that fundamental rights, including intellectual property rights, are fairly balanced against freedom of expression rights.

The study provides a detailed legal analysis that will serve as a firm basis for the further operationalization of these positive State obligations in practice.

1. Introduction

The emergence of the Internet as a dominant medium of contemporary communication has been accompanied by extensive reflection on how this – still relatively new – medium could best be regulated. In the online environment, public and private communications are largely intermediated by private actors, with the result that regulatory control is – in practice – no longer the preserve of the State. Traditional regulatory measures are supplemented by privatized law enforcement measures, prompting questions – if not fears – concerning the effectiveness, transparency and reviewability of such privatized measures. The compliance of such measures with recognized human rights standards is also a source of concern. It is unclear to what extent and how international human rights standards – with their traditional focus on State obligations – should be repurposed in order for them to govern the activities of the actors behind privatized enforcement measures.

Against the backdrop of technological change, the perceived shortcomings of traditional, State-dominated regulatory techniques are well-documented: formal, slow, rigid, lacking insights or participation by key stake-holders, etc. Such shortcomings explain the appeal of an alternative regulatory technique – self-regulation – that has increasingly been espoused in respect of online activities and communication. Self-regulation is typically by a sector, for a sector. When it functions well, it usually boasts flexibility, speed and a strong participatory dynamic that can ensure the centrality of sectoral specificities in the self-regulatory enterprise. When it does not function well, however, it is often found wanting in terms of transparency, implementation machinery and procedural safeguards.

The term, self-regulation, carries different nuances and associations (see further, Section 1.2.1, below), but it essentially entails sectoral attempts to self-organise for self-regulatory purposes, in a way that complements, or obviates the need for, formal legislation. This understanding of the term emphasizes the sectoral dimension and a commonality of purpose shared by (a number of) actors in a given sector.

As such, self-regulation can be distinguished from particularized or privatized measures of law enforcement undertaken by individual actors. Self-regulation could be seen as a sort of collaborative privatized enforcement. Where self-regulatory systems are in place, privatized enforcement would be expected to comply with the standards governing those systems, insofar as the actors in question are subject to the system.

With its primary focus on the online environment, this study embraces instances of both self-regulatory and other privatized enforcement measures alternately and as relevant, with a view to examining their compatibility with States' obligations under international and European human rights law.

Self-regulation continues to be a prevalent form of regulation in the online environment. Self-regulation and private ordering more generally can constitute effective ways of fulfilling public policy objectives such as the protection of minors and the minimization of harms.[1] However, it is also clear that the use of this regulatory strategy by governments and internet service providers often entails the enforcement of rules that interfere with fundamental rights

[1] See: M. Price & S. Verhulst, *Self-Regulation and the Internet*, (Kluwer Law International 2004); OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (Paris, 2011).

of internet users (e.g. blocking of content, access, sharing of personal data), thus limiting the effective exercise of fundamental rights by internet users. As has been noted in academic literature and in policy documents, this can lead to privatized censorship of online material and other interferences with fundamental rights without a clear legal way of redress or appropriate safeguards such as due process.[2] For instance, an agreement between broadband providers and the music industry to cut off internet access of allegedly infringing users will severely limit the free exercise of the right to freedom of expression of those affected. And if such an agreement would also involve more extensive practices with regard to the handing over of, or the creation of a database of, the personal data of the alleged infringers, it would also interfere with their rights to privacy and data protection.

Indeed, the use of self-regulatory or privatized enforcement measures in the online environment can give rise to various legal issues that affect the fundamental rights of internet users. First, privatized enforcement by internet service providers, without state involvement, can interfere with the effective exercise of fundamental rights by internet users. Such interference may, on occasion, be disproportionate, but there are legal complexities involved in determining the precise circumstances in which that is the case. This is because, for instance, the private entities can themselves claim protection under the fundamental rights framework (specifically, the protection of property and the freedom to conduct a business).

Second and related, the role of public authorities in the development of self-regulation in view of certain public policy objectives requires carefully assessment.[3] The fundamental rights framework puts limitations on government regulation that interferes with fundamental rights. Such limitations involve, in the first place, the (negative) obligation for States not to interfere with fundamental rights. Interferences have to be prescribed by law, pursue a legitimate aim and be necessary in a democratic society. At the same time, however, States are also under the (positive) obligation to take active measures (i.e., not just refrain from interference) in order to ensure the effective exercise of fundamental rights. Relevant positive obligations tend to be abstract and difficult to operationalize in practice, yet they can be particularly interesting in the context of the impact of private ordering on fundamental rights.

The issues discussed above have been recognized in constitutional law, international law, internet regulation, case law and in legal scholarship,[4] but there is a clear need for a more focused study of the actual limitations on privatized enforcement following from the

[2] See: J. McNamee, 'The Slide from "Self-Regulation" to Corporate Censorship', Brussels, European Digital Rights (EDRI), 2011; I. Brown, 'Internet Self-Regulation and Fundamental Rights' (2010), *Index on Censorship*, Vol. 1; D. Bambauer, 'Orwell's Armchair', (2012) 79 *University of Chicago Law Review* 863; OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, *op. cit.*; D. Tambini *et al.*, *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence* (London, Routledge, 2008); S.F. Kreimer, 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link', (2006) 11 *University of Pennsylvania Law Review*, 155; P.B. Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace', in I.A. Stamatoudi, Ed., *Copyright Enforcement and the Internet* (Alphen aan den Rijn, Kluwer Law International, 2010), pp. 303-320; B.J. Koops *et al.*, 'Should Self-Regulation be the Starting Point?', in B.J. Koops, M. Lips, C. Prins & M. Schellekens, Eds., *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners* (The Hague, T.M.C. Asser Press, 2006), pp. 109–149.

[3] See, Hans-Bredow-Institut, & Institue of European Media Law, Final Report Study on Co-Regulation Measures in the Media Sector, Hamburg/Saarbruken, 2006.

[4] See: D. Tambini *et al*., *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence*, *op. cit.*; C.T. Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (New York, Cambridge University Press, 2011).

fundamental rights framework. The Council of Europe Commissioner for Human Rights has identified this need very forthrightly as follows:

> Member states should stop relying on private companies that control the Internet and the wider digital environment to impose restrictions that are in violation of the state's human rights obligations. To that end, more guidance is needed on the circumstances in which actions or omissions of private companies that infringe human rights entail the responsibility of the state. This includes guidance on the level of state involvement in the infringement that is necessary for such responsibility to be engaged and on the obligations of the state to ensure that the general terms and conditions of private companies are not at variance with human rights standards. State responsibilities with regard to measures implemented by private parties for business reasons, without direct involvement of the state, also need to be examined.[5]

The present study sets out to fill this gap in scholarship and policy-making. It seeks to provide legal guidance for those involved in internet policy discussions on recurrent questions such as the legitimacy and limitations of online self-regulation and privatized enforcement.[6] For instance, the European Commission continues to be involved in a number of such initiatives at the EU level, e.g. the CEO Coalition to make the Internet a better place for kids,[7] and there are various instances of privatized enforcement at the national level that raise pressing questions from a fundamental rights perspective.[8] This study will help those involved to provide constructive input to improve such online regulation and prevent undue interference with the communicative freedoms of internet users.

1.1. Research questions, scope and methodology

The general research question addressed in this study reads as follows:

What legal limitations follow from the fundamental rights framework for self-regulation and privatized enforcement online?

Or, in other words, in which circumstances can State responsibility be engaged as a result of self-regulation or privatized enforcement online? To answer these contiguous questions, the study will be divided into two parts, namely an overview and analysis of the relevant elements in the fundamental rights framework that place limitations on privatized enforcement (Part I) and an assessment of specific instances of self-regulation or other instances of privatized enforcement in light of these elements (Part II). The study will result in a set of conclusions that will contribute to relevant policy-making.

---

[5] Recommendation 14, Council of Europe Commissioner for Human Rights, Recommendations accompanying D. Korff, *The rule of law on the Internet and in the wider digital world*, Issue paper published by the Commissioner for Human Rights (Strasbourg, Council of Europe, 2014), p. 23.

[6] See: OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, *op. cit.*; J. McNamee, 'The Slide from "Self-Regulation" to Corporate Censorship', *op. cit.*

[7] For an overview, see: http://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids.

[8] See the analysis in N-square, *Study on the Scope of Voluntary Law Enforcement Measures Undertaken by Internet Intermediaries* (2012).

Part I will analyze the elements of the fundamental rights framework that are relevant for the study, through an examination of fundamental rights instruments, case law and literature. It will first set out the protection of the communicative freedoms of internet users in view of privatized enforcement measures by internet services. Of particular relevance in this regard are the right to freedom of expression and information, the right to confidentiality of communications and a number of related rights, namely the right to privacy, the right to due process, the right to an effective remedy, the right to (intellectual) property and the freedom to conduct a business. The primary focus will be placed on the European Convention on Human Rights (Articles 6, 8, 10, 11, 13 and Article 1, Protocol 1) and the Charter of Fundamental Rights of the European Union (Articles 7, 8, 11, 12, 16, 17, 47). Reference will also be made to relevant developments in the international human rights framework and fundamental rights protection at the national level.

On this basis, Part I will address the way in which, and under which circumstances, these rights place restrictions on private ordering and the use of self-regulation by public authorities as a regulatory paradigm for the online environment. It will first discuss the possibility, scope and implications of the *horizontal effect* of fundamental rights, i.e., between private parties. Second, it will discuss their implications for the role of the State, and public authorities more generally, to safeguard the free exercise of fundamental rights, including States' *positive obligations* to this end. Pertinent questions in this discussion include: which types of private ordering are permissible, preferable to direct regulation or even expected from the perspective of the fundamental rights framework, as well as the protection of private ordering under the fundamental rights framework itself? The discussion also includes considerations of when such actions are to be deemed to infringe fundamental rights, on what basis, and what the legal consequence of this might be in practice (*actionability*). Finally, a number of *guiding criteria* are identified that can be used to assess specific instances of privatized enforcement in practice.

Part II will use the guiding criteria identified in Part I to analyze a number of known instances of privatized enforcement in the online environment. The focuses of the case-studies are: (1) Non-judicial notice-and-takedown procedures of social networking services; (2) Voluntary use of content-ID tools by hosting providers to avoid liability for illegal content, and (3) Voluntary scanning of private data by online service providers and the subsequent reporting of users to law enforcement agencies. Each of these focuses corresponds to typical situations in which different online actors engage in practices of privatized enforcement in ways that implicate various fundamental rights of users. Against the background of a rigorous analysis of the relevant legal frameworks, the assessment of the legality and proportionality of the privatized enforcement measures used in these selected case studies aims to elucidate the legal issues and problems involved for the benefit of ongoing policy discussions on relevant matters.

The analysis will also be used to illustrate the way to go about such an assessment in future cases, on the basis of the criteria developed in Part I of the study. In other words, it will further develop the list of guiding criteria for the assessment of self-regulation and privatized enforcement in the online environment.

1.2.Conceptual, definitional and terminological considerations

1.2.1. Self-regulation and privatized enforcement

In the context of this study, self-regulation is taken to mean 'pure' self-regulation, i.e., the "control of activities by the private parties concerned without the direct involvement of public authorities",[9] or more forcefully, "a process of self-regulation where the State has no role to play".[10] Other forms of self-regulation exist, which do include government involvement, such as 'enforced self-regulation', 'regulated self-regulation' and 'self-monitoring'. Due to the involvement of government, such systems are more characteristic of co-regulation and are therefore outside the scope of this study.[11]

The European Commission has advocated the use of self-regulatory mechanisms as the most appropriate form of regulating the internet and mobile technologies, due to constant technological developments in those areas. The flexibility of self-regulation is seen as the most suitable means of regulating those particular areas.[12] For instance, the Audiovisual Media Services Directive (Article 4(7)) encourages EU Member States to explore the suitability of self- and/or co-regulatory techniques.[13] Similarly, both the Directive on electronic commerce (Article 16)[14] and the Data Protection Directive (Article 27)[15] have stressed the importance of codes of conduct; approaches which represent a tentative move away from traditional regulatory techniques in the direction of self-regulation.

The 'legitimacy' or 'democratic deficit'[16] argument, however, indicates that self-regulatory mechanisms, which are created and implemented by private actors are less accountable than state bodies which are made up of democratically elected representatives.[17] Monroe Price and Stefaan Verhulst have argued that due to this fact, self-regulatory bodies can never completely replace statutory bodies in the media sector since it is the responsibility of the state to protect fundamental rights.[18]

---

[9] Mandelkern Group on Better Regulation Final Report, 13 November 2001, p. 83.
[10] Hans-Bredow Institut, Regulated Self-Regulation as a Form of Modern Government: Study commissioned by the German Federal Commissioner for Cultural and Media Affairs (Interim Report, October 2001) at 3.
[11] *Ibid.*
[12] See http://ec.europa.eu/information-society/activities/sip/self_regulation/index_en.htm.
[13] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version), [2010] OJ L 95/1.
[14] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17 July 2000, p. 1.
[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995, p. 31.
[16] E. Lievens, P. Valcke & P.J. Valgaeran, 'State of the art on regulatory trends in media - Identifying whether, what how and who to regulate in social media', Interdisciplinary Centre for Law & ICT (ICRI) December 2011, EMSOC, available at http://emsoc.be/wp-content/uploads/2012/01/State-of-the-art-on-regulatory-trends-in-media.Identifying-whether-what-how-and-who-to-regulate-in-social-media.pdf.
[17] C.T. Marsden, "Co and Self-Regulation in European Media and Internet Sectors: The Results of Oxford University Study", in C. Möller & A. Amouroux, Eds., *The Media Freedom Internet Cookbook* (Vienna, OSCE, 2004), at 93.
[18] See M. Price & S. Verhulst, "In Search of the Self: Charting the course of selfregulation on the Internet and global environment", in C. Marsden, *Regulating the global information society* (London, Routledge, 2000), at p. 65.

In a 2011 study of Internet self-regulation, Joe McNamee argues that many of the so-called self-regulatory methods currently used by online intermediaries should more appropriately be referred to as "devolved law enforcement" where private bodies become "the police, judge, jury and executioner with regard to alleged infringements of either the law or of their own terms and conditions which may be stricter than law".[19] Some research has shown that intermediaries adopt these strict practices due to governmental pressure and unclear legal protections.[20] According to McNamee, examples of "devolved enforcement" methods include non-judicial internet filtering and blocking mechanisms.

Privatized enforcement, a term that is recurrent in this study, refers to instances where private parties (voluntarily) undertake law-enforcement measures. This could be seen as a kind of private ordering (the regulation of users' behaviour through contractual or technical measures[21]), based on their own assessment or interpretation of the meaning and requirements of relevant law.

1.2.2. Measures against illegal content

There are four main types of measures that can be taken against unwanted content of any kind, including therefore illegal content: merely cutting off access to selected material (this is usually termed **blocking**); removing the material altogether from the service (**removal**); monitoring the content in order to identify unwanted material (**monitoring**) and taking action against material identified through monitoring in order to then block access to it or remove it (**filtering**).[22]

Although all four enforcement measures are closely related to each other, the distinction is useful from a legal perspective, as it is capable of remaining close to the technical definitions, while also being broad enough to rise above them and focus on the effects that the measures pursue, rather than the means used to achieve them.[23]

The distinction is particularly helpful in the fundamental rights context, as the different types of measures engage different fundamental rights.[24] Blocking and removal measures mainly

---

[19] J. McNamee, 'The Slide from "Self-Regulation" to Corporate Censorship', *op. cit*, at p. 4.

[20] See further, N-square, *Study on the Scope of Voluntary Law Enforcement Measures Undertaken by Internet Intermediaries*, *op. cit*.

[21] For a detailed exploration of relevant issues, see N. Elkin-Koren, 'Copyrights in Cyberspace - Rights without Laws', 73 Chi.-Kent. L. Rev. 1155 (1998), available at: http://scholarship.kentlaw.iit.edu/cklawreview/vol73/iss4/10.

22 See Steering Committee report on filtering, which recognises that content-control technical actions (which it terms "technical filtering measures") may work by either blocking unwanted content or by filtering it away, Council of Europe, "Report by 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, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282008%2937&Ver=add.

23 Opinion of AG Cruz Villalón, case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* 14 April 2011, para. 46.

24 See also Council of Europe Commissioner for Human Rights, "The rule of law on the Internet and in the wider digital world", issue paper, December 2014. Taking a more granular approach that individually assesses different types of blocking and filtering, the paper observes at p. 71 that: "IP address blocking is cheap, non-intrusive and extremely likely to block unrelated content; domain blocking is cheap, non-intrusive and somewhat less likely to block unrelated content; Cleanfeed (a hybrid system developed by British Telecom) is somewhat more intrusive but very narrowly targeted; deep packet inspection is vastly intrusive and a major restriction on privacy rights, but also the most accurate."

risk endangering users' freedom of expression and information, as well as, potentially, the freedom of the intermediary to conduct a business. Monitoring, which necessarily involves the examination of the private communications of innocent bystanders, although certainly capable on creating a chilling effect on freedom of expression, primarily brings users' privacy and data protection into play. Filtering, as the combination of the two, has the potential to endanger both rights. Accordingly, this distinction shall be followed in the sections below.

In the following paragraphs, the concepts of blocking/removal, monitoring and filtering of content will be briefly defined.

1.2.3. Blocking and removal

Blocking and removal require the identification of the material to be blocked through means other than monitoring. This can be achieved, for example, through notification of the unlawful material. Notice-and-take-down regimes in fact rely on exactly such "mere blocking/removal" systems, the "notice" by the right holder or another party being the means by which the illegal content is discovered by the intermediary so that access to it may be denied. Under this sort of scheme, therefore, content cannot be blocked or removed unless it has already been identified and included in a pre-fixed list of undesirable content by the intermediary undertaking the blocking or removal. Blocking/removal lists will vary from intermediary to intermediary, meaning that some material may be blocked or removed by some intermediaries, but not by others. The blocking or removal may take place at the point at which the data is requested or at that at which it is sent and it may involve specifically identified communications, user accounts or entire websites.

Blocking techniques may vary. For example, URL-based blocking compares the website requested by the user with a pre-determined "blacklist" of URLs of objectionable websites selected by the intermediary imposing the blocking. URLs (or uniform resource locators, otherwise known more colloquially as "web addresses") are character strings that constitute a reference (an address) to a resource on the internet and that are usually displayed inside an address bar located at the top of the user interface of web browsers. The blacklist is compiled by collecting the websites that have been deemed block-worthy, usually through notification by interested parties or identification by the intermediary itself. If a webpage matches one of the sites on this list, the dialogue is redirected before the request leaves the private network, usually to a warning page that explains what has happened. As a result, the user is barred from entering the site. "Whitelists" of URL addresses that users are allowed to visit reverse the principle: instead of only letting users through to URLs that are not on the list, they only permit access to URLs that are on the list. Another blocking technique is offered by IP-based blocking. This operates in a similar manner to URL blocking, but uses IP (Internet Protocol) addresses, i.e., the numerical labels assigned to devices, such as computers, that participate in a network that uses the internet protocol for communication. IP-based blocking has a higher chance of resulting in unintended "over-blocking" than targeted URL blocking as a result of IP sharing, as a given unique IP address may correspond to multiple URLs of different websites hosted on the same server.[25]

Removal of content rests on very similar assumptions as those just identified for the case of

25 Council of Europe, "Report by 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, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282008%2937&Ver=add.

blocking with two major differences. Firstly, while blocking can be "target specific", meaning that it is able to discriminate for which users the content should be available and for which it should be blocked (a feature also known as "withholding"), removal is more definitive in character and general in scope. Once specific content is removed from a server it will not be available to any user. Secondly, removals can logically be executed only by the party who has control over the hosting service where the content is stored, namely a hosting provider itself. Access providers cannot proceed to real removal of content, although they can implement very pervasive blocking to similar effects.

1.2.4. Monitoring

Monitoring refers to the act of proactively seeking out infringing content. Monitoring is therefore the main element that distinguishes blocking/removal from filtering. Monitoring techniques vary depending on a number of factors: the type of content sought, the type of intermediary (access provider or hosting provider), the type of communications (plain text or encrypted) and the nature of the communication (client-server, peer-to-peer, etc.). Monitoring tools such as content control software can be placed at various levels in the internet structure: they can be implemented by all intermediaries operating in a certain geographical area or only by one or some of those intermediaries; they can be applied to all of the customers of an intermediary or only to some of them (for example only to customers originating form country X); they can look only for certain content which is commonly transmitted through specific services (such as illegal file sharing through peer-to-peer networks) or indiscriminately to all content.

Monitoring by hosting providers usually requires the use of software (such as web crawlers) that searches for the presence on their servers of specifically identified illegal content. The identification of the illegal content can be performed in different ways: sometimes through lists of protected subject matter submitted to the intermediary by right-holders, while in other cases specific "strings" or other indicators of content illegality are employed (e.g. the use of specific words or expressions that may be indicators of crime-related activities). Monitoring can also operate before (or at the same time as) the content is uploaded.

Monitoring by access providers requires the use of software that is able to "intercept" and "read" the information transmitted over their network's segment. This practice can be particularly invasive of users' privacy and communications. The internet, technically speaking, is a packet-switched network which means, *inter alia*, that a single piece of information, say an e-mail, in order to go from point A to point B, is subdivided in many small packets of information and sent along, usually, the most de-congested route.[26] This means that different packets of the same communication commonly travel through different routes to reach point B. It follows that in order to intercept potentially infringing content it is not possible or sufficient to monitor only one segment of the network, since the content, or part thereof, could follow a different route. Once all the packets of a single data transfer are gathered and aligned following the right sequence, it becomes possible to "read" the content of the data transfer by looking into the "packets body". This is usually done employing techniques of "Deep Packet Inspection", whereby not only the "headers" of the data packet are read (this is a necessary part of any data transmission over the Internet), but also the "body" of the data packet is read in order to identify the content.

26 See T. Margoni & M. Perry, 'Deep pockets, packets, and safe harbours' (2013) (74: 6) *Ohio State Law Journal* 1195.

1.2.5. Filtering

Filtering is comparable to blocking in respect of the final result, however it goes one step further. It takes a more proactive approach to the identification of objectionable material through incorporating monitoring as the unwanted content identification technique. Instead of waiting for unlawful content to be reported, intermediaries may decide to, or be required to, attempt to locate as many instances of illegal content as possible. Modern technical instruments of identification and surveillance greatly assist such efforts. For example, fingerprinting technology uses a condensed digital summary of each piece of protected content, e.g. of a videoclip (a "fingerprint" of the content), to identify it among all the traffic uploaded on a hosting website or flowing through a network, by means of comparison with a pre-existing extensive reference database of all fingerprints collected by the intermediary applying the filtering. Right-holders who want to protect their works online can contribute a fingerprint of that work to the database before an infringement is ever identified. If a match is detected, the offending material is removed. One such system is YouTube's Content ID (see further, Case study 2, below). This creates an ID file for copyright-protected audio and video material whose owners have signed up for participation and stores it in a database. When a video is uploaded onto the platform, it is automatically scanned against the database. If a match is found, the video is flagged as a potential copyright violation. The content owner then has the choice of muting the video, blocking it from being viewed, tracking the video's viewing statistics or monetising the video by adding advertisements.[27]

The advantage of filtering technology over simple blocking is that the detection of unwanted material is automated, simplifying the enforcement process. Content filtering can also allow for certain types of content to be removed from pages that are intentionally allowed by URL blocking. A major disadvantage is that it involves the monitoring of the totality of the information passing through the intermediary, which may impose a big technical and financial burden on it. This burden may be manageable for platforms that simply have to examine content uploaded to their own servers, but can pose difficulties for internet access providers, which would have to inspect each and every communication passing through their networks to achieve the same effect. As AG Cruz Villalón observed, to be effective, filtering must be "systematic, universal and progressive".[28] There is an added level of difficulty if the intermediary has to break encryption measures in order to identify the content and evaluate its blockworthiness. As a result of all these obstacles filtering systems are not infallible. An independent test of YouTube's Content ID in 2009, for example, uploaded multiple versions of the same song to YouTube and concluded that, while the system was "surprisingly resilient" in finding copyright violations in the audio tracks of videos, it could be easily sabotaged and was not intelligent enough to detect useful meta-information, such as repeat infringers.[29]

Filtering can also risk falling foul of legal limitations. This was, for example, found to be the case with the filtering technology that Belgian collective management society SABAM

27 YouTube, "How Content ID Works", available at: https://support.google.com/youtube/answer/2797370?hl=en.
28 Opinion of AG Cruz Villalón, case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* 14 April 2011, para. 48.
29 Electronic Frontier Foundation, "Testing YouTube's Audio Content ID System", 29 April 2009, available at: https://www.eff.org/deeplinks/2009/04/testing-youtubes-aud.

(*Société d'Auteurs Belge – Belgische Auteurs Maatschappij*) attempted to impose on internet access provider Scarlet. As the *Cour d'appel de Bruxelles* noted, the system advocated by SABAM would require the processing of all electronic communications passing via the intermediary's services, both incoming and outgoing, in particular those involving the use of peer-to-peer software, of all of the ISP's customers, *in abstracto* and as a preventive measure, exclusively at the cost of the ISP and for an unlimited period, in order to identify on its network the movement of electronic files containing a copyrighted work and the subsequent blocking of the transfer of such files. The Court of Justice of the European Union (hereafter, CJEU) found such a system incompatible with a fair balance with competing fundamental rights, including the freedom of business of the intermediary, the freedom of information of its users and their rights to privacy and data protection.[30]

It is important to note that filtering need not necessarily be done by machine: if an intermediary engages humans to manually monitor all communications passing through its systems for unwanted material, that operation would equally qualify as filtering.[31]

30 Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011.

31 "Principles for User Generated Content Services", available at: www.ugcprinciples.com.

PART I

2. Overview and analysis of relevant fundamental rights instruments

2.1. The Council of Europe

The Council of Europe has adopted a number of treaties that are concerned with the protection of the rights to freedom of expression and information, as well as their corollary media freedom, both off- and online. The European Convention on Human Rights (ECHR) is the oldest and most important of those treaties. Other treaties with relevant thematic focusess have been elaborated by the Council of Europe; they are all inspired by the ECHR and are complementary to it. Examples of those treaties include: the Convention on Cybercrime and its Amending Protocol, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems; the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and its Additional Protocol regarding supervisory authorities and transborder data flows; the European Convention on Transfrontier Television (as amended); the Framework Convention for the Protection of National Minorities, etc.

The following section will provide a panorama of the most relevant ECHR provisions that safeguard communication rights. Relevant provisions of other Council of Europe treaties and other normative standards will be introduced into the analysis later in the study, as appropriate.

The term "communication rights" is not enshrined in leading international human rights treaties. It is a term of convenience that covers a cluster of rights that are indispensable for the effective exercise of communicative freedoms. These rights typically include the right to freedom of expression, freedom of assembly and association, privacy, etc. They also include the right to an effective remedy whenever the aforementioned rights have been violated, as well as various process rights that serve to guarantee procedural fairness and justice. These communication rights can also be described, more broadly, as participatory rights as their exercise is a prerequisite for effective participation in democratic society. Whatever the preferred collective term, it is clear that the interplay between these rights is increasing as society steadily becomes more and more digitized.[32]

2.1.1. The European Convention on Human Rights

Before we proceed to a detailed analysis of the ECHR provisions that protect communication rights, we must first examine the interpretative principles that allow the European Court of

[32] See further: D. Mac Síthigh, 'From freedom of speech to the right to communicate' in Price, M.E., Verhulst, S.G. & Morgan, L. (eds.) (2013) *Routledge Handbook of Media Law*, London & New York: Routledge, 2013, pp. 175-191, at 186-187.

Human Rights (hereafter, ECtHR) – which is not known for its "abstract theorising"[33] – to shape the future contours of communication rights: the margin of appreciation doctrine; the practical and effective doctrine; the living instrument doctrine and the positive obligations doctrine. Each will now be dealt with briefly in turn and the positive obligations doctrine, because of its centrality in this study, will be examined in greater detail in Section 3, below.

Under the margin of appreciation doctrine, which has an important influence on how the ECHR is interpreted at national level, States are given a certain amount of discretion in how they regulate expression.[34] That discretion is, however, supervised by the ECtHR and when exercising its supervisory function, the Court does not take the place of the national authorities, but reviews decisions taken by them (see further, below).

According to the practical and effective doctrine, all rights guaranteed by the ECHR must be "practical and effective" and not merely "theoretical or illusory".[35] In other words, the rights must be real and meaningful – they cannot be mere paper tigers. This means that it is essential that rights be interpreted in a way that is informed by contextual specificities. Whether the exercise of a right is effective or whether an interference with a right is justified, will depend on the broader circumstances of the case.

Under the "living instrument" doctrine,[36] the ECHR "must be interpreted in the light of present-day conditions".[37] The aim of this "dynamic and evolutive"[38] interpretive approach is to guard against the risk that the Convention would ever become static. The doctrine applies to both the substance and the enforcement processes[39] of the Convention and even to institutional bodies which did not exist and were not envisaged at the time of its drafting.[40]

The essence of the positive obligations doctrine is that in order for States to ensure that everyone can exercise all of the rights enshrined in the ECHR in a practical and effective manner, it is often not sufficient for State authorities merely to honour their negative obligation not to interfere with those rights. Positive – or affirmative – action may be required on the part of States in some circumstances, with possible implications for relations between private parties or individuals.

2.1.2. Freedom of expression

[33] A. Mowbray, "The Creativity of the European Court of Human Rights", *Human Rights Law Review* 5: 1 (2005), 57-79, at 61.
[34] Initially developed in the Court's case-law, a reference to the doctrine will be enshrined in the Preamble to the ECHR as soon as the Convention's Amending Protocol No. 15 enters into force.
[35] *Airey v. Ireland*, 9 October 1979, Series A no. 32, para. 24.
[36] For an overview of the historical development of the "living instrument" doctrine (including recent developments) by the European Court of Human Rights, see: A. Mowbray, "The Creativity of the European Court of Human Rights", *op. cit*.
[37] *Tyrer v. the United Kingdom*, 25 April 1978, Series A no. 26, para. 31; *Matthews v. the United Kingdom* [GC], no. 24833/94, ECHR 1999-I, para. 39.
[38] *Stafford v. the United Kingdom* [GC], no. 46295/99, ECHR 2002-IV, para. 68; *Christine Goodwin v. the United Kingdom* [GC], no. 28957/95, ECHR 2002-VI, para. 74. Mowbray has pointed out that the Court has recently been making references to the "living instrument" doctrine and the "dynamic and evolutive" interpretative approach pretty much interchangeably: *op. cit.*, p. 64.
[39] *Loizidou v. Turkey (preliminary objections)*, 23 March 1995, Series A no. 310, para. 71.
[40] *Matthews v. the United Kingdom, op. cit*., para. 39.

Article 10 ECHR is the centrepiece of European-level protection for the right to freedom of expression. It reads:

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 10(1) sets out the right to freedom of expression as a compound right comprising the freedom to hold opinions and to receive and impart information and ideas. As such, there are three distinct components to the right, corresponding to different aspects of the communicative process, i.e., holding views, receiving and sending content. These rights are prerequisites for the functioning of media and journalism, including in an online environment.

Article 10(1), ECHR, countenances the possibility for States to regulate the audiovisual media by means of licensing schemes. This provision was inserted as a reaction to the abuse of radio, television and cinema for Nazi propaganda during the Second World War. Article 10(2) then proceeds to trammel the core right set out in the preceding paragraph. It does so by enumerating a number of grounds, based on which the right *may* legitimately be restricted, *provided that* the restrictions are *prescribed by law* and are *necessary in a democratic society*. It justifies this approach by linking the permissibility of restrictions on the right to the existence of *duties* and *responsibilities* which govern its exercise. Whereas the right to freedom of expression is regarded as being subject to general duties and responsibilities, the European Court of Human Rights sometimes refers to the specific duties or responsibilities pertaining to specific professions, e.g., journalism, education, military service, etc. The Court has held that those duties or responsibilities may vary, depending on the technology being used. In light of the casuistic nature of the Court's jurisprudence on duties and responsibilities and in light of its ongoing efforts to apply its free expression principles to the Internet (see further, below), it is only a matter of time before it begins to proffer indications of the nature of Internet actors' duties and responsibilities in respect of freedom of expression.

Notwithstanding the potential offered by Article 10(2) to restrict the right to freedom of expression on certain grounds (although legitimate restrictions must be narrowly drawn and interpreted restrictively), as the European Court of Human Rights famously stated in its *Handyside* judgment, information and ideas which "offend, shock or disturb the State or any sector of the population" must be allowed to circulate in order to safeguard the "pluralism, tolerance and broadmindedness without which there is no 'democratic society'".[41] The question of how far the *Handyside* principle actually reaches in practice is very pertinent as regards online content due to the widely-perceived permissiveness of the Internet as a medium. It is of particular relevance for Case study 1, below.

[41] *Handyside v. the United Kingdom*, 7 December 1976, Series A no. 24, para. 49.

Aside from the permissible grounds for restrictions set out in Article 10(2), ECHR, the right to freedom of expression may also be limited, or rather denied, on the basis of Article 17, ECHR ('Prohibition of abuse of rights').[42] Whenever it has been applied by the Court, this article has been used consistently to ensure that Article 10 protection is not extended to racist, xenophobic or anti-Semitic speech; statements denying, disputing, minimising or condoning the Holocaust, or (neo-)Nazi ideas. This means that in practice, sanctions for racist speech do not violate the right to freedom of expression of those uttering the racist speech. In other words, national criminal and/or civil law can legitimately punish racist speech. However, the criteria used by the Court for resorting to Article 17 (as opposed to Article 10(2)) are unclear, leading to divergent jurisprudence.[43]

The scope of the right to freedom of expression is not only determined by the permissible restrictions set out in Articles 10(2) and 17, ECHR. It is also determined by the interplay between the right and other Convention rights, including the right to privacy, freedom of assembly and association and freedom of religion.

The European Court of Human Rights has developed a standard test to determine whether Article 10, ECHR, has been violated. Put simply, whenever it has been established that there has been an interference with the right to freedom of expression, that interference must first of all be prescribed by law. In other words, it must be adequately accessible and reasonably foreseeable in its consequences. Second, it must pursue a legitimate aim (i.e., correspond to one of the aims set out in Article 10(2)). Third, it must be necessary in a democratic society, i.e., it must correspond to a "pressing social need", and it must be proportionate to the legitimate aim(s) pursued.

The margin of appreciation doctrine, sketched above, is relevant for the assessment of the necessity in democratic society of a measure interfering with the right to freedom of expression. The extent of the discretion afforded to States under the doctrine varies depending on the nature of the expression in question. Whereas States only have a narrow margin of appreciation in respect of political expression, they enjoy a wider margin of appreciation in respect of public morals, decency and religion. This is usually explained by the absence of a European consensus on whether/how such matters should be regulated. When exercising its supervisory function, the European Court of Human Rights reviews the decisions taken by the national authorities pursuant to their margin of appreciation under Article 10, ECHR. Thus, the Court looks at the expression complained of in the broader circumstances of the case and determines whether the reasons given by the national authorities for the restriction and how they implemented it are "relevant and sufficient" in the context of the interpretation of the Convention.

2.1.3. Other communication rights

[42] It reads: "Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention".

[43] H. Cannie & D. Voorhoof, "The Abuse Clause and Freedom of Expression in the European Human Rights Convention: An Added Value for Democracy and Human Rights Protection?", 29 *Netherlands Quarterly of Human Rights* (No. 1, 2011), pp. 54-83; D. Keane, "Attacking hate speech under Article 17 of the European Convention on Human Rights", 25 *Netherlands Quarterly of Human Rights* (No. 4, 2007), pp. 641-663.

Besides the right to freedom of expression, the other main *substantive* communication rights featuring in this study are the right to privacy and the right to freedom of assembly and association.

The right to privacy is safeguarded in Article 8, ECHR, which is entitled, 'Right to respect for private and family life'. It reads:

> 1 Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The growing case-law of the European Court of Human Rights on Article 8 shows attention for relational and informational dimensions to privacy, as well as awareness of contextual specificities and implications of digitised and online environment. The scope of Article 8 also includes the protection of personal data. Relevant case-law also transcends the limitations of the phrase "interference by a public authority" and covers relations between individuals and third-party actors (see further, below).

The right to freedom of assembly and association is safeguarded by Article 11, ECHR:

> 1 Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.
>
> 2 No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. This article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.

Unlike Articles 8 and 10, this provision does not include an explicit reference to "interference by public authority" and the Court's relevant case-law repeatedly and explicitly acknowledges that third parties (and not only State authorities) can interfere with the right to freedom of assembly, e.g., in the context of demonstrations and counter-demonstrations.[44] Rights of access to public spaces and quasi-public spaces (e.g., a privately-owned shopping mall) for communicative purposes have also been considered in the Court's case-law and these cases concerning physical access raise interesting questions for virtual/online access.[45]

The right to protection of property is not enshrined in the text of the Convention, but in Article 1 of Protocol 1 (A1P1) to the Convention:

[44] *Plattform "Ärzte für das Leben" v. Austria,* 21 June 1988, Series A no. 139.
[45] *Appleby and Others v. the United Kingdom*, no. 44306/98, ECHR 2003-VI.

> Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.
>
> The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.

Although the right is set out in A1P1, it is nevertheless to be seen as an integral part of the Convention. Relevant case law of the ECtHR clarifies that the notion of property includes intellectual property[46] and the relationship of the right to intellectual property to the right to freedom of expression has been considered in a number of recent cases.[47]

Alongside these *substantive* communication rights, various *process* rights are also important, such as the right to a fair trial and, even more pertinently, the right to an effective remedy. Those rights are guaranteed in Articles 6 and 13, respectively.

Article 6 concerns the determination of an individual's "civil rights and obligations" and "any criminal charge" against him/her. In these contexts, "everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law" (Article 6(1)). The presumption of innocence applies to charges for criminal offences (Article 6(2)). As will be argued below, the process values prioritized in the case-law pertaining to Article 6, also apply *mutatis mutandis* to administrative redress mechanisms that operate outside the formal institutional structures of the State, e.g., self-regulatory bodies.

Article 13, for its part, reads:

> Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

The undertaking by the ECHR to ensure that individuals have effective remedies for breaches of their human rights is one of the most important features of the Convention and its adjudicative mechanism. It is a stand-alone guarantee that usefully complements the Court's pledge to ensure that ECHR-rights are effective in practice.

2.1.4. Consolidating communication rights in an online environment

The particular importance of the media for democratic society has been stressed repeatedly by the Court. The media can make important contributions to public debate by (widely) disseminating information and ideas and thereby contributing to opinion-forming processes within society. As the Court consistently acknowledges, this is particularly true of the audiovisual media because of their reach and impact. The Court has traditionally regarded the audiovisual media as more pervasive than the print media. It has yet to set out a clear policy line for online media, but it has ventured to say, in 2013, that "the choices inherent in the use of the internet and social media mean that the information emerging therefrom does not have

[46] *Anheuser-Busch Inc. v. Portugal* [GC], no. 73049/01, para. 72, ECHR 2007-I.
[47] *Ashby Donald and Others v. France*, no. 36769/08, 10 January 2013; *Fredrik Neij and Peter Sunde Kolmisoppi v. Sweden* (dec.), no. 40397/12, ECHR 2013.

the same synchronicity or impact as broadcasted information".[48] It continued by stating that notwithstanding "the significant development of the internet and social media in recent years, there is no evidence of a sufficiently serious shift in the respective influences of the new and of the broadcast media in the [United Kingdom] to undermine the need for special measures for the latter".[49] The media can also make important contributions to public debate by serving as fora for discussion and debate. This is especially true of new media technologies which have considerable potential for high levels of individual and group participation.[50]

Furthermore, the role of "public watchdog" is very often ascribed to the media in a democratic society. In other words, the media should monitor the activities of governmental authorities vigilantly and publicise any wrong-doing on their part. In respect of information about governmental activities, but also more broadly in respect of matters of public interest generally, the Court has held time and again that: "[n]ot only do the media have the task of imparting such information and ideas: the public also has a right to receive them".[51]

To date, the European Court of Human Rights has engaged meaningfully with the Internet generally,[52] and the specific features of the online communications environment in particular, in a surprisingly limited number of cases.[53] It has focused on the duty of care of Internet service providers,[54] the added value of online newspaper archives for news purposes[55] and interestingly, the challenges of sifting through the informational abundance offered by the Internet.[56] How the Court dealt with the final point is of interest:

> "It is true that the Internet is an information and communication tool particularly distinct from the printed media, in particular as regards the capacity to store and transmit information. The electronic network serving billions of users worldwide is not and potentially cannot be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned. [...]."[57]

[48] *Animal Rights Defenders International v. the United Kingdom*, para. 119.
[49] *Ibid*.
[50] See further in this connection: *Ahmet Yildirim v. Turkey*, no. 3111/10, ECHR 2012.
[51] *The Sunday Times v. the United Kingdom (no. 1)*, 26 April 1979, Series A no. 30, para. 65.
[52] T. Murphy and G. Ó Cuinn, "Works in Progress: New Technologies and the European Court of Human Rights", 10(4) *Human Rights Law Review* (2010), pp. 601-638, at p. 636; European Court of Human Rights (Research Division), *Internet: case-law of the European Court of Human Rights* (Strasbourg, Council of Europe, 2011); European Court of Human Rights (Press Unit), *Fact sheet – New technologies* (Strasbourg, Council of Europe, February 2015).
[53] T. McGonagle, 'User-generated Content and Audiovisual News: The Ups and Downs of an Uncertain Relationship', in S. Nikoltchev, Ed., *Open Journalism, IRIS plus* 2013-2 (Strasbourg, European Audiovisual Observatory), pp. 7-25.
[54] *K.U. v. Finland*, no. 2872/02, ECHR 2008, para. 49.
[55] *Times Newspapers Ltd. (nos. 1 & 2) v. the United Kingdom*, nos. 3002/03 and 23676/03, ECHR 2009, para. 45; *Węgrzynowski and Smolczewski v. Poland*, no. 33846/07, 16 July 2013.
[56] *Editorial Board of* Pravoye Delo *and Shtekel v. Ukraine*, no. 33014/05, ECHR 2011.
[57] *Ibid*., para. 63.

The Court made these observations in a case involving a newspaper that, owing to a lack of funds, "often reprinted articles and other material obtained from various public sources, including the Internet".[58] In short, the Court is calling for a rethink of familiar principles of media freedom and regulation in the expansive, global context of the Internet.

Again, these findings by the Court focus on journalists and professional media, but in light of the expanding understandings of the roles such professions play, they are also of relevance for other actors. This reading is confirmed by the reference to the importance of the Internet "for the exercise of the right to freedom of expression generally".[59] The Court has repeatedly recognised that besides professional journalists and media, individuals, civil society organisations, whistle-blowers and academics can all make valuable contributions to public debate, thereby playing a role similar or equivalent to that traditionally played by the institutionalised media.

From the cited passage, above, it is clear that the Court places the onus on states' authorities to develop a legal framework clarifying issues such as responsibility and liability. It is unclear, however, to what extent an equivalent self-regulatory framework would suffice. The Court has held in other case law that self- and co-regulatory mechanisms can suffice, provided they include effective guarantees of rights and effective remedies for violations of rights.[60] In any case, it is clear that "the State cannot absolve itself from responsibility by delegating its obligations to private bodies or individuals".[61] As will be explained in Section 3.4, below, State responsibility can, in certain circumstances, be triggered indirectly by the acts or omissions of private bodies.

In its *Ahmet Yildirim v. Turkey* judgment of 18 December 2012, the Court recognised in a very forthright way the importance of the Internet in the contemporary communications landscape. It stated that the Internet "has become one of the principal means for individuals to exercise their right to freedom of expression today: it offers essential tools for participation in activities and debates relating to questions of politics or public interest".[62]

This recognition clearly places great store by the participatory dimension of free expression. The Court found that a measure resulting in the wholesale blocking of Google Sites in Turkey "by rendering large quantities of information inaccessible, substantially restricted the rights of Internet users and had a significant collateral effect".[63] The interference "did not satisfy the foreseeability requirement under the Convention and did not afford the applicant the degree of protection to which he was entitled by the rule of law in a democratic society".[64] In addition, it produced arbitrary effects.[65] Furthermore, the Court found that "the judicial-review procedures concerning the blocking of Internet sites are insufficient to meet the

[58] *Ibid*., para. 5.
[59] *Times Newspapers Ltd v. United Kingdom (nos. 1 and 2)*, no. 3002/03 and 23676/03, § 27, 10 March 2009.
[60] For details and analysis, see: Hans-Bredow-Institut for Media Research, University of Hamburg, *Study on Co-Regulation Measures in the Media Sector*, Final Report, Study for the European Commission, Directorate Information Society and Media, 2006, pp. 147-152. See, in particular, the analysis of *Peck v. the United Kingdom*, no. 44647/98, ECHR 2003-I, paras. 108 & 109.
[61] *Costello-Roberts v. the United Kingdom*, 25 March 1993, Series A no. 247-C, para. 27; see also, *Van der Mussele v. Belgium*, 23 November 1983, Series A no. 70, paras. 29-30.
[62] *Ahmet Yildirim v. Turkey*, *op. cit*., para. 54.
[63] *Ibid*., para. 66. See also the later judgment of *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, § 64, ECHR 2015.
[64] *Ibid*., para. 67.
[65] *Ibid*., para. 68.

criteria for avoiding abuse, as domestic law does not provide for any safeguards to ensure that a blocking order in respect of a specific site is not used as a means of blocking access in general".[66] This reasoning suggests that the Court would also disapprove of other intrusive or overly-broad blocking techniques, such as those detailed in the Introduction to this study.

In the case of *Delfi AS* v. *Estonia*,[67] the Estonian courts held a large online news portal liable for the unlawful third-party comments posted on its site in response to one of its own articles, despite having an automated filtering system and a notice-and-takedown procedure in place. The Grand Chamber of the Court found that this did not amount to a violation of Article 10 ECHR. The judgment has proved very controversial, particularly among free speech advocates, who fear that such liability would create pro-active monitoring obligations for Internet intermediaries, leading to private censorship and a chilling effect on freedom of expression.

The contentious nature of the judgment stems from a number of the Court's key lines of reasoning therein. First, the Court took the view that "the majority of the impugned comments amounted to hate speech or incitements to violence and as such did not enjoy the protection of Article 10".[68] By classifying the comments as such extreme forms of speech, the Court purports to legitimize the stringent measures that it sets out for online news portals to take against such manifestly unlawful content. The dissenting judges object to this approach, pointing out that "[t]hroughout the whole judgment the description or characterisation of the comments varies and remains non-specific"[69] and "murky".[70]

Secondly, the Court endorses the view of the Estonian Supreme Court that Delfi could have avoided liability if it had removed the impugned comments "without delay".[71] This requirement is problematic because, as pointed out by the dissenting judges, it is not linked to notice or actual knowledge[72] and paves the way to systematic, pro-active monitoring of third-party content.

Thirdly, the Court underscored that Delfi was "a professionally managed Internet news portal run on a commercial basis which sought to attract a large number of comments on news articles published by it".[73] The dissenting judges aptly argued that the economic activity of the news portal does not cancel out the potential of comment sections for facilitating individual contributions to public debate in a way that "does not depend on centralised media decisions".[74]

Fourthly, the Court failed to appreciate or articulate the broader ramifications of far-reaching Internet intermediary liability for online freedom of expression generally. It was at pains to stress that "the case does not concern other fora on the Internet where third-party comments can be disseminated, for example an Internet discussion forum or a bulletin board where users can freely set out their ideas on any topics without the discussion being channelled by any input from the forum's manager; or a social media platform where the platform provider

[66] *Ibid*.
[67] *Delfi AS* v. *Estonia* [GC], no. 64569/09, ECHR 2015.
[68] *Ibid*., para. 136.
[69] *Ibid*., Joint Dissenting Opinion of Judges Sajó and Tsotsoria, para. 12.
[70] *Ibid*., Joint Dissenting Opinion, para. 13.
[71] *Ibid*., para. 153.
[72] *Ibid*., Joint Dissenting Opinion, para. 8.
[73] *Ibid*., para. 144.
[74] *Ibid*., Joint Dissenting Opinion, para. 39 and 28.

does not offer any content and where the content provider may be a private person running the website or a blog as a hobby".[75] The dissenting judges again took great exception to this line of reasoning, describing it as an exercise in "damage control".[76]

While the above developments remain quite tentative in the case-law of the European Court of Human Rights, they are more advanced in other Council of Europe standard-setting activities.[77] Although such standard-setting work, notably by the organisation's Committee of Ministers[78] and Parliamentary Assembly,[79] is not legally-binding, it is politically persuasive and offers a number of advantages over treaty-based approaches.[80] It can, for example, engage with issues in a more detailed way than is possible either in treaty provisions or case-law or monitoring pursuant to treaty provisions. It can also address issues that have not arisen in case-law, but are nevertheless relevant. In the same vein, it can identify and address emergent or anticipated developments, thereby ensuring a dynamic/modern approach to relevant issues.

Standard-setting by the Committee of Ministers includes a number of focuses that are relevant for the present study, e.g.: self-regulation concerning cyber content; human rights and the rule of law in the Information Society; freedom of expression and information in the new information and communications environment; the public service value of the Internet; respect for freedom of expression and information with regard to Internet filters; network neutrality; freedom of expression, association and assembly with regard to privately operated Internet platforms and online service providers; human rights and search engines; human rights and social networking services, and risks to fundamental rights stemming from digital tracking and other surveillance technologies. These normative texts generally explore their subject matter in an expansive way, while grounding the exploration in relevant principles that have already been established by the ECtHR. As such, the texts tease out the likely application of key legal principles to new developments, thereby also giving an indication of the likely content of specific State obligations in respect of those principles. Their role and influence, while not legally-binding, can nevertheless be seen as instructive.

Thus, the Committee of Ministers has highlighted the gravity of violations of Articles 10 and 11, ECHR, "which might result from politically motivated pressure exerted on privately operated Internet platforms and online service providers".[81] It has insisted that the use of filters be strictly in accordance with Articles 10 and 6, ECHR, and specifically be targeted, transparent and subject to independent and impartial review procedures. It encourages member states and the private sector to "strengthen the information and guidance to users who are subject to filters in private networks, including information about the existence of, and reasons for, the use of a filter and the criteria upon which the filter operates".[82] It has also

[75] *Ibid*., para. 116.
[76] *Ibid*., Joint Dissenting Opinion, para. 9.
[77] See generally: W. Benedek and M.C. Kettemann, *Freedom of expression and the Internet* (Strasbourg, Council of Europe Publishing, 2013).
[78] S. Nikoltchev & T. McGonagle, Eds, *Freedom of Expression and the Media: Standard-setting by the Council of Europe, (I) Committee of Ministers - IRIS Themes* (Strasbourg, European Audiovisual Observatory, 2011).
[79] S. Nikoltchev & T. McGonagle, Eds., *Freedom of Expression and the Media: Standard-setting by the Council of Europe, (II) Parliamentary Assembly - IRIS Themes* (Strasbourg, European Audiovisual Observatory, 2011).
[80] T. McGonagle & K. de Beer, "*A brave new media world?* Een kritische blik op het nieuwe mediabeleid van de Raad van Europa", 22 *Mediaforum* 2010-5, pp. 146-156.
[81] CM Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers (2011), para. 7.
[82] CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters, Guidelines, section III.

called on member states to "promote transparent self- and co-regulatory mechanisms for search engines, in particular with regard to the accessibility of content declared illegal by a court or competent authority, as well as of harmful content, bearing in mind the Council of Europe's standards on freedom of expression and due process rights".[83] Finally, in the present string of examples, the Committee of Ministers has stated that social networking services should refrain from "the general blocking and filtering of offensive or harmful content in a way that would hamper its access by users";[84] develop and communicate editorial policies about "inappropriate content", in line with Article 10, ECHR,[85] and "ensure that users are aware of the threats to their human rights and able to seek redress when their rights have been adversely affected".[86] It has called on member states to "encourage the establishment of transparent co-operation mechanisms for law-enforcement authorities and social networking services", which "should include respect for the procedural safeguards required under Article 8, Article 10 and Article 11", ECHR. [87]

2.2.The European Union

The European Union, too, has adopted an array of texts that govern media, journalistic and Internet freedom and communication rights generally. As will be seen below, there is a degree of alignment between Council of Europe and European Union approaches to media freedom and regulation.

2.2.1. The Charter of Fundamental Rights of the European Union

Since the entry-into-force of the Lisbon Treaty, the Charter of Fundamental Rights of the European Union has acquired the same legal status as the EU treaties, thereby enhancing its relevance. The Charter's provisions "are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law" (Article 51(1)). "They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties" (*ibid*.).

The Charter's provisions which "contain principles may be implemented by legislative and executive acts taken by institutions, bodies, offices and agencies of the Union, and by acts of Member States when they are implementing Union law, in the exercise of their respective powers" (Article 52(5)). However, they shall be "judicially cognisable only in the interpretation of such acts and in the ruling on their legality" (*ibid*.).

It is important to ensure that the human rights standards elaborated by the Council of Europe and the European Union are (broadly) consistent or equivalent. Divergence would be detrimental to legal certainty and predictability, and indeed to the overall European human rights project. For these reasons, the Charter expressly stipulates that insofar as the Charter contains rights that correspond to those safeguarded by the ECHR, "the meaning and scope of those rights shall be the same as those laid down by" the ECHR (Article 52(3)). This reference to the ECHR includes the case-law of the European Court of Human Rights.[88] If the

[83] CM/Rec(2012)3 on the protection of human rights with regard to search engines, para. 8.
[84] CM/Rec(2012)4 on the protection of human rights with regard to social networking services, para. 11.
[85] *Ibid*., para. 10. See also para. 3.
[86] *Ibid*., para. 15.
[87] *Ibid*., para. 11.
[88] Commentary of the Charter, p. 400; Presidium, CHARTE 4473/1/00, CONVENT 49.

European Union eventually accedes to the ECHR, this substantive alignment will be formalised and strengthened. In the same vein, insofar as the Charter recognises fundamental rights resulting from the constitutional traditions common to EU Member States, those rights shall be interpreted in harmony with those traditions (Article 52(4)).

Even though there is deliberate congruence between the ECHR and the Charter, the latter also purports to offer added value beyond that of the former. The following table indicates selected differences of approach taken under the Charter to the main rights discussed in this study.

Description of right	**ECHR**	**Charter**	**Description of right**
Freedom of expression	Art. 10	Art. 11	Freedom of expression and information
Right to respect for private and family life	Art. 8	Art. 7	Right to private and family life
		Art. 8	Right to protection of personal data
Freedom of assembly and association	Art. 11	Art. 12	Freedom of assembly and association
Right to property	Art. 1, Protocol 1	Art. 17(2)	Right to intellectual property
Right to an effective remedy	Art. 13	Art. 47	Right to an effective remedy and to a fair trial
Right to a fair trial	Art. 6		

In most of these examples, the difference of approach involves a highlighting or an unpacking of particular principles identified in the case-law of the European Court of Human Rights and their explicit recognition in a legally-binding text. Examples include the reference to media pluralism as part of the right to freedom of expression and the recognition of a right to protection of personal data as a stand-alone right (as opposed to one subsumed in a more general right to privacy).[89]

Article 11 of the Charter reads:

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
> 2. The freedom and pluralism of the media shall be respected.

Article 11 of the Charter should be interpreted consistently with Article 10, ECHR, and relevant case-law of the European Court of Human Rights. The text of Article 11 of the Charter is modelled on Article 10, ECHR, but is more succinctly formulated and one of its purported aims is to provide a modern interpretation of Article 10, ECHR. Its added value – explicit mention of media freedom and pluralism – is diluted by the weak formula ("shall be respected") adopted.[90] By way of contrast, as will be seen below, the European Court of Human Rights has held that the State is the ultimate guarantor of pluralism, especially in the audiovisual media sector, thereby recognizing a far-reaching positive obligation for the

[89] For commentary, see the relevant chapters in S. Peers *et al*. (eds.), *The EU Charter of Fundamental Rights: A Commentary*, Oxford: Hart Publishing 2014, in particular: L. Woods, 'Article 11 – Freedom of Expression and Information', p. 311-340; H. Kranenborg, 'Article 8 – Protection of Personal Data', p. 223-265.
[90] See further, T. McGonagle, *Minority Rights, Freedom of Expression and of the Media: Dynamics and Dilemmas,* Vol. 44, School of Human Rights Research Series (Antwerp, etc., Intersentia, 2011), p. 464.

State.[91] Notwithstanding the weak formulation in Article 11(2) of the Charter, there is currently an ostensible political interest within the EU in developing the media pluralism agenda.[92]

The Charter also includes a number of relevant rights that are not (explicitly) enshrined in the ECHR, such as the right to protection of personal data (Art. 8), the freedom to conduct a business (Art. 16), the right to intellectual property (Art. 17(2)) and the right of access to services of general economic interest (Art. 36). These newly recognized rights and/or explicit emphases must be factored into the balancing of human/fundamental rights, as relevant. As such, they serve to adjust and expand the parameters of the balancing exercise that has traditionally taken place in the context of the ECHR.

The right to protection of personal data has been at the heart of a string of recent judgments by the CJEU, which have played an important role in consolidating the fundamental nature of the right. In its *Digital Rights Ireland* judgment, for instance, the CJEU ruled that the Data Retention Directive[93] was invalid, *inter alia*, because the Directive failed to lay down clear and precise rules governing the extent of the interference with the fundamental rules enshrined in Articles 7 and 8 of the Charter".[94] Moreover, the Court found that the Directive did not "provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of" data "retained by providers of publicly available electronic communications services or of public communications networks".[95]

Likewise, in its *Schrems* judgment,[96] the CJEU ruled that the European Commission's so-called "Safe-Harbour" Decision[97] was invalid. The case concerned the ability of national supervisory authorities to examine "the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection". The CJEU restated the principles that had formed the mainstay of its reasoning in its *Digital Rights Ireland* judgment.[98]

The *Google Spain* judgment is another CJEU judgment that has helped to undergird the status of the rights to privacy and data protection, albeit in a way that: (i) departs from prior case-law by both the CJEU and the European Court of Human Rights concerning the fair balance principle, and (ii) is detrimental to the right to freedom of expression. The case focused on the question of whether a right exists to have one's name delisted from the search results

[91] *Informationsverein Lentia and Others v. Austria*, 24 November 1993, Series A no. 276, para. 38.
[92] See: "A free and pluralistic media to sustain European democracy", Report of the High Level Group on Media Freedom and Pluralism, January 2013; responses to public consultation on the Report's Recommendations.
[93] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54.
[94] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, para. 65.
[95] *Ibid*., para. 66.
[96] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015.
[97] European Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.
[98] Case C-362/14, *Schrems*, *op. cit*., paras. 91-94.

generated by a search engine on the grounds of the rights to privacy and data protection. The CJEU concluded, *inter alia*, that:

> As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.[99]

The CJEU does countenance an exception, i.e.: "if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question".[100] Nevertheless, this exception seems flimsy, given that the Court, after making a cursory reference to the fair balance between this "interest"[101] and the fundamental rights of the data subject to privacy and data protection, went on to insist that the latter "as a rule" override the former. This approach gives short shrift to the right to freedom of expression, which has equal value to other human rights, according to the European Court of Human Rights. These critical arguments have been developed in greater detail elsewhere by Stefan Kulk and Frederik Zuiderveen Borgesius, who are also critical of one of the corollaries of the judgment, *viz.* that search engine operators have been thrust into the role of having to carry out this balancing exercise.[102] This is an example of private ordering involving fundamental rights.

The freedom to conduct a business is of particular interest in the present study due to potential tensions with the right to freedom of expression. The CJEU held in its *Sky Österreich GmbH* judgment that the freedom to conduct a business "is not absolute, but must be viewed in relation to its social function".[103] As such, it "may be subject to a broad range of interventions on the part of public authorities which may limit the exercise of economic activity in the public interest".[104] As with other rights and freedoms protected by the Charter, any limitation on exercise of the freedom to conduct a business "must be provided for by law and respect the essence of those rights and freedoms and, in compliance with the principle of proportionality, must be necessary and actually meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others".[105] The Court went on to stress that the "safeguarding of the freedoms protected under Article 11 of the Charter undoubtedly constitutes a legitimate aim in the general interest [...], the importance of which in a democratic and pluralistic society must be stressed in particular [...]".[106]

Another noteworthy difference of approach between the ECHR and the Charter is that the former refers to the "duties and responsibilities" that govern the exercise of the right to freedom of expression. This is a unique provision as the reference is not part and parcel of

---

[99] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014, para. 99.
[100] *Ibid.*
[101] *Ibid.*, para. 81.
[102] S. Kulk and F.Z. Borgesius, "Google Spain v. González: Did the Court Forget about Freedom of Expression?", 5 *European Journal of Risk Regulation* (No. 3, 2014), 389-398.
[103] Case C-283/11, *Sky Österreich GmbH v. Österreichischer Rundfunk*, 22 January 2013, para. 45.
[104] *Ibid.*, para. 46.
[105] *Ibid.*, para. 48.
[106] *Ibid.*, para. 52.

any other rights guaranteed by the ECHR. By way of contrast, Article 11 of the Charter does not contain an equivalent reference, but the preamble to the Charter states: "Enjoyment of these rights [i.e., the rights set forth in the Charter] entails responsibilities and duties with regard to other persons, to the human community and to future generations". This is more far-reaching and has implications for a broader range of rights, including in an online context.

The rights enshrined in the Charter must be respected in secondary EU legislation, which operates at a level below the Charter. The implications of this for a selection of directives governing the liability of online intermediaries will be examined in more detail the next sub-section.

2.2.2. The EU legal framework for intermediary liability

In any Europe-focused discussion on self-regulation and privatised enforcement online, the EU's legal framework on the liability of internet intermediaries cannot be omitted. Although it is concerned exclusively with State-imposed liability and court-ordered measures imposed on unwilling internet intermediaries, these provisions can nevertheless shed valuable light on the situation involving similar measures undertaken by such providers of their own accord. This section will proceed to examine the intersection of the law of fundamental rights with the current European enforcement framework as it pertains to public authorities, with a view to illuminating the situation concerning self-regulation and private enforcement.

The EU has developed a piecemeal harmonised framework for intermediary liability. The main bulk of this can be found in its Copyright,[107] Enforcement[108] and E-Commerce Directives.[109] While the Copyright and Enforcement Directives require Member States to ensure that right holders are in a position to apply for injunctions against intermediaries whose services are used by a third party to infringe a copyright, related right or other intellectual property right, the E-Commerce Directive sets limitations on the type of obligations that can be imposed on intermediaries. These Directives will be examined in greater detail, below. The analysis will focus mostly on legal provisions concerning the legality under EU law of court orders imposing injunctive measures on internet intermediaries for enforcement purposes, as these provide the clearest indications of the legality of enforcement measures undertaken voluntarily by intermediaries. It should be noted that the EU framework revolves primarily around intellectual property law and in particular copyright, however many of the conclusions drawn below will have equal applicability in other areas of law. The case of IP is nevertheless particularly interesting as concerns court-ordered measures, given that, as we shall see below, Member States are obligated under EU law to provide IP rights holders with the possibility of applying for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right. This means that the limitations that arise from fundamental rights hold strong even in

[107] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10 (Copyright Directive).
[108] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights [2004] OJ L 157/45 (Enforcement Directive).
[109] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), [2000] OJ L 178/1.

the face of a positive State obligation to ensure enforcement.[110] At the same time, it should be kept in mind that, beyond the context of the harmonised European framework for injunctions in the enforcement of IP, national rules apply, which can result in different standards for the different EU Member States.

Recital 59 of the Copyright Directive makes the observation that in many cases online intermediaries are best placed to bring infringing activities occurring on their digital premises to an end. On this basis, it suggests that right-holders should be given the possibility of applying for an injunction against any intermediary that carries a third party's infringement of protected work or other subject-matter in a network. Article 8(3) of the Copyright Directive explicitly instructs Member States to "ensure that rightsholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right". The 2004 Enforcement Directive reinforces this obligation in Article 11 *in fine*, which refers to the Copyright Directive and repeats the order, expanding it to all intellectual property rights. Recital 23 of the latter indicates the discretion left to the Member States in this area regarding the exact parameters of such measures: "The conditions and procedures relating to such injunctions", it says, "should be left to the national law of the Member States."

The E-Commerce Directive's immunities for intermediaries do not interfere with this framework. Section 4 of the E-Commerce Directive prohibits liability under certain clearly circumscribed circumstances for certain activities or functions performed by online intermediaries, namely "mere conduit" (Article 12), "caching" (Article 13) and "hosting" (Article 14). Each of these conditional liability exemptions, otherwise known as "safe harbour" or "immunity" provisions, is governed by a separate set of conditions that must be met before the intermediary may benefit. Significantly, while the provisions of the Enforcement and Copyright directives focus only on the infringement of intellectual property rights by third parties, the E-Commerce Directive's safe harbours are cross-cutting. The safe harbours are thus intended to function as holistic tools, equally applicable to all different types of illegal online activity, from copyright or trademark infringement to unfair competition and from child pornography to defamation.[111] However, the E-Commerce Directive's safe harbours are limited only to liability in the strict sense, i.e., for monetary damages. All three contain express permissions in their final paragraphs regarding the imposition of any kind of injunctive order on the providers of information society services by "courts and administrative authorities" to "terminate or prevent an infringement". Member States are also permitted to establish "procedures governing the removal or disabling of access to information" stored by host providers.[112]

This does not mean that all injunctive orders imposing enforcement measures against intermediaries are permitted: a significant limitation on the permissible scope of injunctions is imposed by Article 15 of the Directive, which prohibits the imposition of general

[110] Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011, para. 33.

[111] It has been suggested however that the heavy reliance the E-Commerce immunities on the DMCA's safe harbours does indicate a strong leaning towards the copyright perspective, see J. van Hoboken, "Legal Space for Innovative Ordering: On the Need to Update Selection Intermediary Liability in the EU" (2009) 13 *International Journal of Communications Law & Policy* 1.

[112] Art. 14(3), E-Commerce Directive. See also, Recital 45. Article 18 also requires that Member States "ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim injunctions, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved."

obligations on service providers to monitor the information which they transmit or store, or to actively seek facts or circumstances indicating illegal activity when providing the three safe harbour services. The key allowing for the reconciliation of the provisions of the three Directives can be found in the word "general". Recital 47 of the E-Commerce Directive elucidates the meaning of the term in this context by contrasting general monitoring obligations with monitoring obligations imposed in a "specific case" that are issued "by national authorities in accordance with national legislation". Further than this, interpretation has been left to the courts. Orders directed against intermediaries other than those identified in Articles 12-14 are not subject to the Article 15 prohibition of general monitoring orders; although, as the subsequent CJEU case law has demonstrated, limitations may also arise from the primary sources, in particular fundamental rights rules.

In light of the above, it becomes clear that injunctions imposing technical measures on intermediaries will be difficult to keep within the boundaries of Article 15 of the E-Commerce Directive. In *L'Oréal v. eBay,*[113] a trademark case and the earliest CJEU judgment on injunctions against intermediaries, the Court confirmed that injunctions aimed at bringing an end to an infringement, as well as preventing further infringements may be imposed on intermediaries regardless of any liability of their own. Such injunctions must be "effective and dissuasive" and the national rules governing them must "designed in such a way that the objective pursued by the Directive may be achieved."[114] At the same time, however, the measures they impose must be "fair and proportionate and must not be excessively costly."[115] They must also "not create barriers to legitimate trade".[116] This is a repetition of the lattice of contradictory obligations Member States must respect in the enforcement of intellectual property rights outlined in Article 3 of the Enforcement Directive.

To reconcile these conflicting obligations, as stated in *Promusicae*, when several rights and interests are at stake, a "fair balance" must be struck.[117] That ground-breaking decision dealt with the counter-balancing of the fundamental rights of property, including intellectual property (as protected by Article 17(2) of the Charter), and the right to effective judicial protection on the one hand (Article 47 of the Charter) and the protection of personal data and private life (Articles 7 and 8 of the Charter) on the other hand. The Court ruled that "the authorities and courts of the Member States must not only interpret their national law in a manner consistent with [the EU] directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality."[118]

What measures pass this delicate balancing test? In the twin *Sabam* cases, *Scarlet*[119] and *Netlog,*[120] the CJEU took a hard stance against filtering. *L'Oréal v. eBay* had already confirmed that the active monitoring of all the data of each of the intermediary's customers is excluded by Article 15 of the E-Commerce Directive.[121] This conclusion was then repeated in

[113] Case C-324/09, *L'Oréal v eBay,* 12 July 2011.
[114] *L'Oréal v eBay,* para. 136.
[115] *L'Oréal v eBay,* para. 139.
[116] *L'Oréal v eBay,* para. 140.
[117] Case C-275/06, *Promusicae*, 29 January 2008.
[118] *Promusicae*, para. 68.
[119] Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011.
[120] Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, 16 February 2012.
[121] *L'Oréal v eBay,* para. 139.

Scarlet. That case was an extreme one, which involved a request for the imposition, in defence of the claimants' copyright, on an internet access provider of a filtering system geared at identifying copyright-protected works exchanged on the provider's networks and blocking their transfer. Here, the Court went on to find that, even absent Article 15, such a burdensome request would also be illegal under the EU's fundamental rights framework. The general conciliatory rule of a "fair balance" here too took central stage: after noting that copyright is protected under Article 17(2) of the Charter, the Court emphasised that this does not mean that it is inviolable and must be absolutely protected. Instead, the freedom of the intermediary to conduct a business (Article 16 of the Charter), the rights of its customers to the protection of their personal data (Article 8 of the Charter) and their freedom to receive and impart information (Article 11 of the Charter) were identified as counterbalancing rights that may set a limit to copyright enforcement. The Court noted that the requested injunction would require that ISP to install a complicated, costly, permanent computer system at its own expense which would constitute an unreasonable interference with the intermediary's freedom to conduct its business. It would also involve the systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent, those IP addresses being protected personal data. The interference with users' freedom of information was identified on the basis that the system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. The same conclusion was also reached a few months later in *Netlog,* this time with regard to a hosting service provider.[122]

The two *Sabam* rulings were especially significant with regard to establishing fundamental rights as an essential part of the intermediary liability discussion and relevant criteria in solving the tensions between copyright and other rights and interests. They thus confirm the *Promusicae* approach of identifying the limits of enforcement not in secondary legislation, but in the primary sources. This raises the question of whether Article 15 of the E-Commerce Directive is replaceable by fundamental rights legislation: is the provision merely an explicit confirmation for mere conduit, caching and hosting providers of a limitation that would apply anyway as a result of constitutional considerations? The CJEU rulings would seem to suggest that this will often be the case, which in turn would mean that the restrictions of Article 15 will often apply beyond the limited scope that it reserves for itself. In light of *Scarlet*, Dommering concluded that, beyond the vertical harmonisation that obliges Member States to keep their national copyright laws consistent with the harmonised EU copyright framework, the CJEU is aiming at a horizontal harmonisation of copyright law that places it on a level playing field within an autonomous EU fundamental rights framework. In this way, the questions of intellectual property, privacy and the free flow of information are forced to constantly play off each other, shuffling against one another until each slips into its natural resting place, which will differ in each instance, depending on the particular circumstances of each individual case.[123]

---

[122] *Netlog* based the interference with the protection of personal data on "the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users" that the requested system would involve. Such information connected with those profiles was deemed to be protected personal data because, in principle, it allows those users to be identified.

[123] E.J. Dommering, "De Zaak Scarlet/Sabam: Naar een Horizontale Integratie van het Auteursrecht" (2011) 2 *AMI* 49. This interpretation would be in line with the current tentative reconsideration, at least among academics, of the internalisation of the tension between copyright and competing rights, in view of its escalation, brought about by the digital era, beyond the capacity of copyright's internal safeguards, in favour of the construction of a broader conceptual arena where conflicting rights can openly vie against each other on equal terms, see L.C. Torremans, Ed., *Intellectual Property and Human Rights* (2nd ed.) (Wolters Kluwer, 2008);

It should be noted that the injunctions requested in *Sabam*, which would have involved the installation of a filtering mechanism for all electronic communications, both incoming and outgoing, of for all of Scarlet's customers, *in abstracto* and as a preventive measure, at the expense of the ISP and for an unlimited period of time, were strikingly broad. The ruling does not provide answers with regard to orders imposing narrower filtering obligations.[124] That said, it is hard to envision a filtering tool that would not necessarily involve general monitoring, particularly given that in order to be effective, filtering has to be systematic, universal and progressive, bringing it out of proportion with its aims.[125] Filtering after all, by the very definition of the word, necessarily involves examining all communications in order to identify and "filter out" the objectionable ones. So, while in *L'Oréal* the Court explicitly permitted the imposition of measures seeking to prevent future infringements, pre-emptive action against illegality from unknown sources would nevertheless probably be excluded, as this will often amount to *de facto* general monitoring, there being no other way to stop infringing activity, the existence of which intermediaries cannot otherwise become aware of without outside assistance.[126]

The *Sabam* rulings confirmed the conclusions drawn earlier by commentators that the imposition of an obligation for online intermediaries to carry out prior control by means of the installation of a filtering system would be of dubious legality under the EU rules. Court-ordered filtering, although not in principle forbidden, may only be imposed after a careful consideration of its implications for competing rights and interests that will necessarily always exclude its imposition.[127] It is interesting to note that this is despite the fact that the national legal orders are bound by an obligation to provide recourse to injunctions to IP rights holders. It also worth mentioning that, although the above analysis has focused on injunctive orders imposing enforcement measures, the same fundamental rights-derived limitations that exclude general monitoring will also apply to attempts by courts to impose liability for monetary damages on providers that do not adopt enforcement measures. So, for example, the French *Cour de cassation* in two rulings on "*L'affaire Clearstream*" and "*Les dissimulateurs*" on 12 July 2012[128] found that "stay-down" obligations, that result in liability for a provider if, following a notice of an infringement by a right holder, it does not take measures to prevent the future reposting of the infringing content, may not be imposed as they would be impossible to obey without general monitoring. Rights holders must therefore monitor the content of websites themselves and notify intermediaries of each new infringement of protected content that they detect, if they wish to have it removed.

R. Burrell and A. Coleman, *Copyright Exceptions: The Digital Impact* (Cambridge University Press 2005); T. Dreier, 'Balancing Proprietary and Public Domain Interests: Inside or Outside of Proprietary Rights?' in R. Dreyfuss *et al*., Eds., *Expanding the Boundaries of Intellectual Property – Innovation Policy for the Knowledge Economy* (Oxford University Press 2001); P.B. Hugenholtz & M. Senftleben, "Fair Use in Europe – In Search of Flexibilities" (2012) Amsterdam Law School Legal Studies Research Paper No. 2012-39.

[124] S. Kulk & F. Borgesius, "Filtering for Copyright Enforcement in Europe after the Sabam Cases" (2012) 34(11) *EIPR* 791.

[125] Opinion of AG Cruz Villalón, case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* 14 April 2011, para. 48.

[126] T. Verbiest, G. Spindler *et al*., "Study on the Liability of Internet Intermediaries", Markt/2006/09/E, 12 November 2007; "EU Study on the Legal Analysis of A Single Market for the Information Society – New Rules for a New Age?" (November 2009), Chapter 6: "Liability of Internet Intermediaries", available online.

[127] C. Angelopoulos, "Filtering the Internet for Copyright Content in Europe" *IRIS plus* 2009-4.

[128] Cour de cassation (Première chambre civile), *La société Google france c/ La société Bach films,* Arrêt n° 831 du 12 juillet 2012; Cour de cassation (Première chambre civile) *La société Google France c/ La société Bac films,* Arrêt n° 828 du 12 juillet 2012.

Naturally, the fact that such broad monitoring measures are off-bounds for courts formulating injunctive orders does not in itself mean that intermediaries are also prohibited from voluntarily adopting them. Nevertheless, this analysis does suggest that caution and careful consideration might be necessary with regard to possible interferences by intermediaries with the rights of others.

If general monitoring and accordingly filtering may not be imposed by State authorities on intermediaries, what orders may be issued against intermediaries by the courts? Following on the above logic, injunctions ordering the suppression of specific and clearly identifiable people, websites or content that have been found to contain illicit information could be deemed acceptable. Insightfully, in *Scarlet,* AG Cruz Villalón pointed out that filtering and blocking mechanisms, although closely related to each other as to the objectives they pursue, differ essentially as to their nature. They consequently carry very different legal implications (see the Introduction above).[129] And indeed, in *L'Oréal* the Court suggested the suspension of the perpetrator of the infringement as an example of a measure that would reconcile all competing interests. This followed the suggestion by AG Jääskinen of a "double requirement of identity", according to which where the infringing third party is the same and the right infringed is the same, an injunction may be issued ordering the termination of the account of the user in question.[130] This would satisfy the balance between too lax and too aggressive an enforcement of intellectual property rights, between, to use the simile made by the AG, the Scylla of allowing the rampant infringement of copyright and the Charybdis of infringing the rights of users and intermediaries.[131]

It should be noted that, even if this logic is accepted, courts must tread carefully, as even this suggestion is not without its problems: depending on whether the words "perpetrator" and "infringing third party" here are understood to refer to the actual person committing the infringement or simply the account they happen to hold while executing it, the measure may go beyond mere blocking and require filtering software that could run afoul of Article 15 of the E-Commerce Directive.[132] It is interesting that the wording in the AG's Opinion ("closing the client account of the user") and that of the Court ("suspend the perpetrator") suggest different conclusions.

Other considerations should also give pause. For example, it should be noted that even mere blocking can have more extensive repercussions than intended: blocking entire domains, for example, risks collateral damage in the form of disallowing access to fully legal content that happens to be hosted at the same address.[133] More significantly yet, a clear distinction between blocking and filtering cannot be made, given that even cases of targeted and therefore "specific" blocking, will often necessitate the "filtering" of identifying data that help locate the content and differentiate it from other material may be required, if not the processing of the content itself. So, for instance, URL-based blocking which compares the website requested by the user with a pre-determined "blacklist" of URLs of objectionable websites will result in the indiscriminate processing of all URLs passing through the filter, even if only few of these are subsequently blocked. Other measures, such as the termination

[129] Opinion of AG Cruz Villalón, case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* 14 April 2011, para.46.
[130] Opinion of AG Jääskinen, Case C-324/09, *L'Oréal v eBay,* 9 December 2010, para. 182.
[131] Opinion of AG Jääskinen, Case C-324/09, *L'Oréal v eBay,* 9 December 2010, para. 171.
[132] B. Clark & M. Schubert, "Odysseus between Scylla and Charybdis? The ECJ Rules in *L'Oréal v eBay"* (2011) 6(12) JIPLP 880.
[133] M. Horten, *A Copyright Masquerade* (Zed Books, 2013), p. 27.

of an identified user-account, will not pose such problems. Great care is needed in establishing that measures that might at first sight appear to be sufficiently "specific" are indeed so. In any case, what is clear is that if an enforcement measure is specific enough to be imposed on an intermediary as an injunctive order by a court, that intermediary should certainly be able to implement it voluntarily if it chooses.

In *UPC Telekabel Wien*,[134] the CJEU further made clear that the required specificity is limited to the object of the blocking order, i.e., the injunction must target identifiable websites. Blocking injunctions do not need to be specific with regard to the measures the intermediary must adopt to achieve the blocking result. Instead, the courts may leave this decision to the intermediary, as long as it has the opportunity to avoid coercive penalties for breach of the injunction by showing that it has taken all reasonable measures. In choosing such reasonable measures, the intermediary must make sure that it does not disproportionately infringe users' rights. According to the Court, as a result of the fair balance principle, a measure taken by an intermediary will be reasonable if "those measures have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right, that being a matter for the national authorities and courts to establish".[135]

The *Telekabel* case is especially significant as it seems to favour a horizontal applicability of end-users' fundamental rights on an internet provider's legitimate scope of activity. According to the Court, "when the addressee of an injunction such as that at issue in the main proceedings chooses the measures to be adopted in order to comply with that injunction, he must ensure compliance with the fundamental right of internet users to freedom of information."[136] Although in the same decision the Court also insists on the importance of the State providing a possibility for judicial review of the implementing measures taken by the intermediary, this wording seems to strongly suggest that the burden of observing fundamental rights rests on the intermediary as well. If this interpretation is to be accepted, the Court's reasoning is noteworthy: although starting from an examination of the submitted request for a preliminary ruling on the extent of the negative obligations incumbent on the courts as public authorities to refrain from vertically imposing injunctions on intermediaries that infringe either their own rights or those of their users, the CJEU jumps to the horizontal obligation of the intermediary itself to respect the fundamental rights of others – a paradigm shift quite remarkable in its breadth. According to this thinking, internet access providers cannot act indiscriminately with regard to enforcement measures, but must take into account the fundamental rights of end-users, including their rights to freedom of expression and privacy. This obligation persists, irrespective of the fact that they are also under an obligation to adopt an enforcement measure as a result of the injunction imposed on them, just as, as noted above, public authorities are obliged to respect fundamental rights of users and intermediaries, while also owing right-holders injunctive relief under EU law. The "fair balance" first identified in *Promusicae* must therefore be respected not only by the State, as follows naturally from the negative dimension of fundamental rights, but also by private entities, at least following a court order to take a measure that has the potential to interfere with the free exercise of the fundamental rights of third parties. No explanation is given regarding the interference of such obligations with the intermediary's freedom to conduct a

[134] Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH*, 27 March 2014.
[135] *Telekabel*, para. 64.
[136] *Telekabel*, para. 55.

business or what the consequences for an intermediary of a court finding of an interference with a user's right might be. For the privatised enforcement and self-regulation, if this interpretation is correct, it cannot be seen as anything short of ground-breaking: the Court has effectively turned vertical effect into horizontal effect, thereby blasting open the doors from the direct application of fundamental rights on relationships between private parties.

Of course, it should be noted that the issue is a complex one, particularly in view of the fact that private entities can themselves claim protection under the fundamental rights framework (e.g., the protection of property and the freedom to conduct a business).

3. Positive State obligations

3.1. Origins of the doctrine

The international legal system for the protection of human rights pivots on the linear relationship between individuals (rights-holders) and States (duty-bearers). The recognition that different types of non-State/private actors should also be (explicitly) positioned within the system has come about in a gradual and frictional manner. And even that reluctant recognition has only been achieved through the dynamic interpretation of existing legal norms and the interplay between those norms and policy-making documents.

All international human rights treaties share the primary objective of ensuring that the rights enshrined therein are rendered effective for everyone. There is also a predominant tendency in international treaty law to guarantee effective remedies to individuals when their human rights have been violated. In order to achieve these dual objectives, it is not always enough for the State to simply refrain from interfering with individuals' human rights: positive or affirmative action will often be required as well. It is therefore important to acknowledge the concomitance of negative and positive State obligations to safeguard human rights. While this acknowledgement typically informs treaty-interpretation, relevant formulae and approaches tend to vary per treaty.

So, in the context of online intermediary self-regulation as well, in addition to the traditional *negative obligations* that bind public authorities, the *positive obligations* of the State to safeguard human rights can mean that public authorities may be obligated to prevent private parties from engaging in different types of behaviour that endanger the fundamental rights of third parties. This can result in restrictions by public authorities on the use of self-regulation as a regulatory paradigm for the online environment.

In the following sections, a sample of international treaties (i.e., the ECHR and the International Covenant on Civil and Political Rights (ICCPR)) will be surveyed to illustrate the different but comparable approaches to ensure that human rights are effective in practice, to the extent that these are relevant to the question of online enforcement through self-regulation.

3.2. The European Convention on Human Rights

The questions of whether or how international human rights treaties protect individuals against the actions of other private persons do not invite straightforward answers. A leading textbook on the ECHR captures the conceptual difficulties involved when it cautions against describing such protection (in the context of the ECHR) as *Drittwirkung*, a doctrine under which "an individual may rely upon a national bill of rights to bring a claim against a private person who has violated his rights under that instrument".[137] Such a "horizontal application of law […] can have no application under the Convention at the international level, because the

[137] (footnote omitted) D.J. Harris, M. O'Boyle, E.P. Bates & C. Buckley, *Law of the European Convention on Human Rights* (3rd ed.) (Oxford, Oxford University Press, 2014), p. 23.

Convention is a treaty that imposes obligations only upon states".[138] It further clarifies that "insofar as the Convention touches the conduct of private persons, it does so only indirectly through such positive obligations as it imposes upon a state".[139]

Article 1, ECHR, obliges States Parties to the Convention to "secure to everyone within their jurisdiction the rights and freedoms" set out in the Convention. The obligation to "secure" these rights is unequivocal and necessarily involves ensuring that the rights in question are not "theoretical or illusory", but "practical and effective" (see above). Against this backdrop and based on an analysis of the Court's relevant case-law, it has been observed that "various forms of positive obligations have been imposed upon different governmental bodies in order to secure a realistic guarantee of Convention rights and freedoms".[140] What exactly a "realistic guarantee" entails is best determined on a case-by-case basis, although certain trends can tentatively be identified per Convention article. The following examples concern Articles 8, 11 and 10, ECHR.

In its *Airey* judgment, the Court stated that "although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life".[141] In *X. & Y. v. The Netherlands*, it supplemented that statement by admitting that such "obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves".[142] This is an important extension of the principle as articulated in anterior case-law; it confirms a degree of horizontal applicability of relevant rights. Yet, the Court "does not consider it desirable, let alone necessary, to elaborate a general theory concerning the extent to which the Convention guarantees should be extended to relations between private individuals *inter se*".[143] Instead, it seems to prefer the case-by-case approach that has come to typify its jurisprudence.

The Court has deliberately adopted similar reasoning regarding the right to freedom of assembly; it held that "genuine, effective freedom of peaceful assembly" cannot:

> be reduced to a mere duty on the part of the State not to interfere: a purely negative conception would not be compatible with the object and purpose of Article 11. Like Article 8, Article 11 sometimes requires positive measures to be taken, even in the sphere of relations between individuals, if need be [...][144]

The pattern of recognising that positive State duties are sometimes necessary in order to render rights effective can also be detected in respect of Article 10. Such positive State duties apply to substantive and procedural matters alike. For instance, when negligibly-funded informational campaigns aiming to influence debate on matters of public interest are pitted against multinational corporations which have vastly superior financial resources, procedural

[138] (footnotes omitted) *Ibid*.
[139] *Ibid*.
[140] A. Mowbray, "The Creativity of the European Court of Human Rights", *Human Rights Law Review* 5: 1 (2005), 57-79, at 78.
[141] *Airey v. Ireland*, *op. cit*., para. 32.
[142] *X and Y v. the Netherlands*, 26 March 1985, Series A no. 91, para. 23.
[143] *VgT Verein gegen Tierfabriken v. Switzerland*, no. 24699/94, ECHR 2001-VI, para. 46.
[144] *Plattform "Ärzte für das Leben*, *op. cit.*, para. 32.

fairness requires that some approximate equality of arms be strived for. In the Court's own words:

> If, however, a State decides to provide such a remedy [against defamation] to a corporate body, it is essential, in order to safeguard the countervailing interests in free expression and open debate, that a measure of procedural fairness and equality of arms is provided for.[145]

Although the Court does not spell out the implications of its pronouncement, it seems logical that it would be for the State to guarantee the requisite measure of procedural fairness and equality of arms.

As regards more substantive concerns, the Court has accepted in principle that positive measures may be required of States in order to give effect to the right to freedom of expression (as with Articles 8 and 11, including the protection of the right in the sphere of relations between individuals[146]), but it has yet to meaningfully explore the practical workings of the principle. For instance, in *Özgür Gündem v. Turkey*, taking as its starting point, "the key importance of freedom of expression as one of the preconditions for a functioning democracy", the Court recognised that:

> Genuine, effective exercise of this freedom does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals [...]. In determining whether or not a positive obligation exists, regard must be had to the fair balance that has to be struck between the general interest of the community and the interests of the individual, the search for which is inherent throughout the Convention.[147]

This recognition amounts to an important statement of principle, even if the Court does immediately go on to concede:

> The scope of this obligation will inevitably vary, having regard to the diversity of situations obtaining in Contracting States, the difficulties involved in policing modern societies and the choices which must be made in terms of priorities and resources. Nor must such an obligation be interpreted in such a way as to impose an impossible or disproportionate burden on the authorities [...].[148]

Owing to the situational diversity across the Council of Europe, States Parties to the ECHR "enjoy a wide margin of appreciation in determining the steps to be taken to ensure compliance with the Convention", subject to the practical and effective doctrine.[149]

In its *Informationsverein Lentia* judgment, the European Court of Human Rights found, seminally, that the State is the ultimate guarantor of pluralism, especially in the audiovisual media sector.[150] The implications of this positive obligation have since been teased out, most

[145] *Steel & Morris v. the United Kingdom*, no. 68416/01, ECHR 2005-II, para. 95.
[146] See, among other authorities, *Fuentes Bobo v. Spain*, no. 39293/98, 29 February 2000, para. 38.
[147] Özgür Gündem *v. Turkey*, no. 23144/93, ECHR 2000-III, para. 43.
[148] *Ibid*. See also *VgT Verein gegen Tierfabriken v. Switzerland (no. 2)* [GC], no. 32772/02, ECHR 2009, paras. 81 and 82.
[149] *Węgrzynowski and Smolczewski v. Poland*, *op. cit*., para. 55.
[150] *Informationsverein Lentia and Others v. Austria*, 24 November 1993, Series A no. 276, para. 38.

notably in *Verein gegen Tierfabriken*[151] and in *Manole & Others v. Moldova*.[152] In *Verein gegen Tierfabriken,* for instance, the Court held that:

> It is true that powerful financial groups can obtain competitive advantages in the areas of commercial advertising and may thereby exercise pressure on, and eventually curtail the freedom of, the radio and television stations broadcasting the commercials. Such situations undermine the fundamental role of freedom of expression in a democratic society as enshrined in Article 10 of the Convention, in particular where it serves to impart information and ideas of general interest, which the public is moreover entitled to receive. Such an undertaking cannot be successfully accomplished unless it is grounded in the principle of pluralism of which the State is the ultimate guarantor. This observation is especially valid in relation to audio-visual media, whose programmes are often broadcast very widely.

It is important to note in this connection the Court's express linking of freedom of expression, democratic society, pluralism and "especially" the audio-visual media, "whose programmes are often broadcast very widely". If the reason for singling out the audiovisual media is the wide reach of their programmes, then these arguments clearly apply *mutatis mutandis* to the Internet.

Notwithstanding the potential of the State's role as the ultimate guarantor of pluralism in democratic society, the positive obligations engendered by that role do not extend to guaranteeing "freedom of forum" [153] or access to a particular medium/service. [154] In *Melnychuk v. Ukraine*, in which a particular form of access - the right of reply, the Court noted that "as a general principle, newspapers and other privately-owned media must be free to exercise editorial discretion in deciding whether to publish articles, comments and letters submitted by private individuals". [155] It acknowledged that, against this background, "exceptional circumstances" may nevertheless arise "in which a newspaper may legitimately be required to publish, for example, a retraction, an apology or a judgment in a defamation case".[156] Situations such as these may, according to the Court, create a positive obligation "for the State to ensure an individual's freedom of expression in such media".[157]

In *Appleby & others v. the United Kingdom*, the applicants argued that the shopping centre to which they sought to gain access should be regarded as a "quasi-public" space because it was *de facto* a forum for communication. The Court held that:

> [Article 10, ECHR], notwithstanding the acknowledged importance of freedom of expression, 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

[151] *VgT, op. cit*., para. 73.
[152] *Manole and Others v. Moldova*, no. 13936/02, ECHR 2009. See, in particular, paras. 98 and 107.
[153] *Appleby & Others v. the United Kingdom*, *op. cit*., para. 47.
[154] *Haider v. Austria*, no. 25060/94, 18 October 1995; *United Christian Broadcasters Ltd. v. the United Kingdom* (dec.), no. 44802/98, 7 November 2000, *Demuth v. Switzerland*, no. 38743/97, ECHR 2002-IX; *VgT v. Switzerland*.
[155] *Melnychuk v. Ukraine*, Decision of inadmissibility of the European Court of Human Rights (Second Section) of 5 July 2005.
[156] *Ibid*.
[157] *Ibid*.

> 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 (Government offices and ministries, for instance). *Where however 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, the Court would not exclude that a positive obligation could arise for the State to protect the enjoyment of Convention rights by regulating property rights.*[158]

Instead, the Court tends to place store by the existence of viable expressive alternatives to the particular one denied. In determining whether alternative expressive opportunities are actually viable in the circumstances of a given case, it is important to be mindful of the Court's *Khurshid Mustafa & Tarzibachi* judgment,[159] in which it correctly rejected the assumption that different media are functionally equivalent. Different media have different purposes and are used differently by different individuals and groups in society: they are not necessarily interchangeable.[160] This is one explanation of why different media are subject to different regulatory regimes.[161]

Further, as regards the viability of an expressive opportunity, it should be recalled that the Court has held (in respect of the right to freedom of association) that an "individual does not enjoy the right [to freedom of association] if in reality the freedom of action or choice which remains available to him is either non-existent or so reduced as to be of no practical value".[162] This finding, which could be applied analogously to the right to freedom of expression, is another illustration of the Court's commitment to its "practical and effective" doctrine.

In light of the *Khurshid Mustafa & Tarzibachi* judgment, the Court tends to consider whether the blocking of access to a particular medium or forum has the effect of depriving someone of a major source of communication and thereby the possibility of participating in public debate.[163] The Court thus found no breach of the applicant's right to freedom of expression in *Akdeniz v. Turkey* after access to two music-streaming websites was blocked on the ground that they were in breach of copyright. The reasoning was that the applicant in the case could "without difficulty have had access to a range of musical works by numerous means without this entailing a breach of copyright rules".[164] Again, the availability of viable expressive alternatives (or, *in casu* viable alternatives for receiving information) was a central consideration for the Court. The case was distinguished from *Ahmet Yildirim v. Turkey* (discussed above) as it involved copyright and commercial speech, as opposed to political speech and the ability to participate in public debate. Member States have a wider margin of appreciation for commercial speech than for political speech.

In *Cengiz & others v. Turkey*, the Court distinguished *Akdeniz* and re-affirmed the reasoning behind its *Ahmet Yildirim* judgment. The *Cengiz* case concerned the blocking of the YouTube

---

[158] (emphasis added) *Appleby and Others v. the United Kingdom*, *op. cit*., para. 47.
[159] *Khurshid Mustafa & Tarzibachi v. Sweden*, no. 23883/06, 16 December 2008, para. 45.
[160] For further analysis, see: T. McGonagle, 'The Council of Europe's standards on access to the media for minorities: A tale of near misses and staggered successes', in Amos, M., Harrison, J. & Woods, L., Eds., *Freedom of Expression and the Media* (Leiden/Boston, Martinus Nijhoff Publishers, 2012), pp. 111-140, at 118-124.
[161] See, as regards Internet, *Węgrzynowski and Smolczewski v. Poland*, *op. cit*.
[162] *Young, James & Webster v. United Kingdom*, Series A, no. 44, 13 August 1981, para. 56.
[163] *Akdeniz v. Turkey* (dec.), no. 20877/10, 11 March 2014.
[164] *Ibid.*

website in Turkey in 2008. This deprived the applicants, who are academics, of an important source of information and ideas and an important outlet for their academic work. As in its *Khurshid Mustafa and Tarzibachi* judgment, the Court recognized that particular media can provide types of information that are of particular interest to certain (categories of) persons.[165] The Court accepted that, given the specific features of YouTube and how the applicants used it, there was no equivalent platform available to them as a result of the blocking measures.[166] The Court found that while the applicants were not directly targeted by the blocking measures, there had nevertheless been an interference with their right to receive and communicate information and ideas.[167] This collateral effect of the impugned measures was an important consideration for the Court in reaching its conclusion that the applicants' right to freedom of expression had been violated.

Perhaps the most far-reaching positive obligation in relation to freedom of expression to be identified by the Court to date concerns the enablement of freedom of expression in a very broad sense. In *Dink v. Turkey*, the Court stated that States are required to create a favourable environment for participation in public debate for everyone and to enable the expression of ideas and opinions without fear. [168] This finding bridges protective and promotional obligations and it contains great potential for further development, including in respect of online communication. Fear, for example of legal liability for third-party content on a hosting provider, can give rise to a chilling effect on free speech and a restriction on public debate. It has been noted that States should, to "comply fully" with Article 10, ECHR, "ensure that they do not place intermediaries under such fear of liability claims that they come to impose on themselves filtering that is appropriate for making them immune to any subsequent accusation but is of a kind that threatens the freedom of expression of Internet users".[169]

Reviewing the foregoing, it can be observed that the Court's recognition of positive State obligations in respect of communication rights is nascent and piecemeal, but steady. The process of recognition will continue to be guided by the living instrument doctrine and the practical and effective doctrine. It will also be driven by the Court's gradual but growing appreciation of the specificities of the online communications environment. At present, the criteria applied by the Court in determining whether a State has failed to honour specific positive obligations remain somewhat unclear, thus making the following clarification very welcome:

> the boundaries between the State's positive and negative obligations under the Convention do not lend themselves to precise definition. The applicable principles are nonetheless similar. Whether the case is analysed in terms of a positive duty on the State or in terms of interference by a public authority which needs to be justified, the criteria to be applied do not differ in substance. In both contexts regard must be had to the fair balance to be struck between the competing interests at stake.[170]

[165] *Cengiz and Others v. Turkey*, *op. cit*., § 51.
[166] *Cengiz and Others v. Turkey*, *op. cit*., § 52.
[167] *Cengiz and Others v. Turkey*, *op. cit*., § 64.
[168] *Dink v. Turkey*, nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, 14 September 2010, para. 137.
[169] E. Montero and Q. Van Enis, "Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: Squaring the circle", *Computer Law & Security Review* 27 (2011) 21-35, at 34.
[170] *VgT (No. 2), op. cit*., para. 82. See also *Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, ECHR 2012, para. 99.

The practical implications of this finding will be teased out in Section 3.4, below. That section will specifically address the question: what positive obligations do States have in respect of interferences with individual communication rights by private parties? First, though, attention will turn to the development of the positive obligations doctrine in the context of the ICCPR.

3.3. The International Covenant on Civil and Political Rights

Under Article 2(1) of the ICCPR,[171] States Parties must "respect" and "ensure" to all individuals subject to their jurisdiction the rights recognised in the Covenant in a non-discriminatory manner. The obligation undertaken by States Parties is therefore twofold. First, "to respect" all of the rights recognised in the ICCPR, States must not violate them. Second, "to ensure" those rights is a more far-reaching undertaking and, according to one leading commentator, it "implies an affirmative obligation by the state to take whatever measures are necessary to enable individuals to enjoy or exercise the rights guaranteed in the Covenant, including the removal of governmental and possibly also some private obstacles to the enjoyment of these rights".[172] The reading of affirmative State obligations into Article 2, ICCPR, is borne out by subsequent paragraphs of the Article and the interpretive clarifications offered, *inter alia*, by the UN Human Rights Committee's General Comment No. 31 – "The Nature of the General Legal Obligation Imposed on States Parties to the Covenant".

Article 2(2) requires States "to take the necessary steps, in accordance with its constitutional processes and with the provisions of the present Covenant, to adopt such laws or other measures as may be necessary to give effect to the rights recognized in the present Covenant". This requirement is "unqualified and of immediate effect".[173] In addition, pursuant to Article 2(3), States "must ensure that individuals also have accessible and effective remedies to vindicate those rights".[174] The envisaged remedies "should be appropriately adapted so as to take account of the special vulnerability of certain categories of person […]".[175]

Specifically regarding the right to freedom of expression (as enshrined in Article 19, ICCPR), the Human Rights Committee's General Comment No. 34 states:

> The obligation to respect freedoms of opinion and expression is binding on every State party as a whole. All branches of the State (executive, legislative and judicial) and other public or governmental authorities, at whatever level – national, regional or local – are in a position to engage the responsibility of the State party. Such responsibility may also be incurred by a State party under some

[171] It reads: "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."
[172] T. Buergenthal, "To Respect and Ensure: State Obligations and Permissible Derogations", in L. Henkin, Ed., *The International Bill of Rights* (New York, Columbia University Press, 1981), pp. 72-91, at 77. Buergenthal also notes that such affirmative obligations could include "providing some access to places and media for public assembly or expression" – *ibid.*
[173] General Comment No. 31 [80] – "The Nature of the General Legal Obligations Imposed on States Parties to the Covenant", 29 March 2004, para. 14.
[174] *Ibid.*, para. 15.
[175] *Ibid.*

> circumstances in respect of acts of semi-State entities. The obligation also requires States parties to ensure that persons are protected from any acts by private persons or entities that would impair the enjoyment of the freedoms of opinion and expression to the extent that these Covenant rights are amenable to application between private persons or entities.[176]

Although the terms "positive obligations" and "affirmative action" do not appear in the text of General Comment No. 34, the last sentence in the cited passage, above, is unambiguous: in certain circumstances, States may have a positive obligation to take measures to prevent violations of individuals' right to freedom of expression by third parties. In light of the General Comment's repeated insistence that the scope of the right of freedom of expression extends to all forms of online communication,[177] there is no doubt that positive State obligations arise in respect of Internet-based communication.

In respect of the right to privacy (as enshrined in Article 17, ICCPR), the Human Rights Committee is even more emphatic about the existence and extent of States' positive obligations, including in the sphere of individual relations. The opening paragraph of the Committee's General Comment No. 16 reads as follows:

> Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour and reputation. In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.[178]

The General Comment further states that "States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant *and to provide the legislative framework prohibiting such acts by natural or legal persons*".[179] Additionally, as "Article 17 affords protection to personal honour and reputation", States are under an obligation to "provide adequate legislation to that end".[180] The importance of redress is also stressed in this connection: "Provision must also be made for everyone effectively to be able to protect himself against any unlawful attacks that do occur and to have an effective remedy against those responsible".[181]

In conclusion, it is clear that the concept of positive State obligations is well-consolidated in the context of the ICCPR, both in theory and in practice, even if the precise term is not used.

---

[176] (footnotes omitted) UN Human Rights Committee, General Comment 34: Article 19 (Freedoms of Opinion and Expression), UN Doc. CCPR/C/GC/34, 12 September 2011, para. 7.
[177] See, for example, paras. 12, 15, 43-45.
[178] United Nations Human Rights Committee, General Comment No. 16 – Doc. No. A/43/40, 28 September 1988, para. 1. See also para. 6.
[179] (emphasis added) *Ibid*., para. 9.
[180] *Ibid*., para. 11.
[181] *Ibid*.

3.4. What positive obligations do States have in respect of interferences with individual communication rights by private parties?

3.4.1. The European human rights framework

As demonstrated in the previous sub-sections, the positive obligations doctrine has developed by accretion and its precise scope and finer details continue to evolve. Besides the doctrinal evolution in the case-law of the ECtHR, it is also instructive to consider the potential guidance offered by relevant standard-setting work by the Council of Europe's Committee of Ministers and relevant case law of the CJEU. For analytical purposes, it is useful to group positive State obligations relating to communication rights online into three categories: preventive, promotional and remedial. These categories are not, however, mutually exclusive. As will be shown, preventive and promotional obligations, for example, overlap to an extent.

3.4.1.1 Preventive obligations

States are required to put in place regulatory frameworks (including legislative frameworks) to ensure the effective exercise of communication rights in the online environment. These frameworks should include legislative frameworks[182] and, more specifically, criminal-law frameworks, as appropriate, for instance for combating child pornography.[183] In respect of medical data, which constitutes "highly intimate and sensitive" data, States must ensure that the law affords "practical and effective protection to exclude any possibility of unauthorised access" to such data.[184] States must ensure that laws not only meet the *Sunday Times* criteria concerning the quality of law (foreseeability and accessibility),[185] but in particular for surveillance of communications, for example, additional criteria apply in the interests of transparency/avoiding chilling effect and to ensure safeguards against various possible abuses.[186]

The obligations described in the previous paragraph exist regardless of the existence of self-regulatory mechanisms. While States may enjoy discretion as to the means they use to fulfil their fundamental rights obligations, they may not delegate those obligations to private parties.[187] Relatedly, these obligations also exist regardless of States' obligations under other international treaties, especially when source of those obligations is an international

[182] *Editorial Board of* Pravoye Delo *and Shtekel v. Ukraine, op. cit.*
[183] *K.U. v. Finland*, *op. cit.*
[184] *I. v. Finland*, no. 20511/03, §§ 38, 39 and 47, 17 July 2008; *Z. v. Finland*, judgment of 25 February 1997, Reports of Judgments and Decisions 1997-I, §§ 95-96.
[185] See also in this connection, Council of Europe Commissioner for Human Rights, Recommendation 16 (2014).
[186] See, in particular, *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 95, ECHR 2006-XI (which summarizes "the minimum safeguards that should be set out in statute law in order to avoid abuses of power"), and generally: *Klaas v. Germany*, 22 September 1993, Series A no. 269; *Kruslin v. France*, 24 April 1990, Series A no. 176-A; *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82. For a detailed discussion of these issues, see: S. Eskens, O. van Daalen and N. van Eijk, *Ten standards for oversight and transparency of national intelligence services*, Amsterdam, Institute for Information Law (IViR), 2015.
[187] *Woś v. Poland*, no. 22860/02, ECHR 2006-VII, *Michaud v. France*, no. 12323/11, ECHR 2012; consider also *Barthold v. Germany*, 25 March 1985, Series A no. 90, *Peck v. the United Kingdom*, *op. cit.*, *Fuentes Bobo*, *op. cit*.

organisation with "equivalent" levels of human rights protection.[188] Thus, EU-law (for example) may neither displace nor dilute positive State obligations identified and developed by the ECtHR pursuant to the ECHR.

3.4.1.2 Promotional obligations

States also have positive obligations to actively promote different values, such as pluralistic tolerance in society and media pluralism. Whereas the role of the State as "ultimate guarantor" of media pluralism has traditionally concerned the audiovisual media sector,[189] it is likely – in light of the living instrument and practical and effective doctrines, that this principle will have to be developed and applied *mutatis mutandis* to the online environment. Similarly, States' positive obligation to ensure an environment that is favourable to freedom of expression[190] necessitates adaptation for optimal realization in the online environment. Etienne Montero and Quentin Van Enis have posited that States' positive obligations, when "[t]ransposed to the digital universe", include the adoption of "a genuinely reassuring framework for intermediaries in order to avoid the private censorship they are liable to effect through fear of liability action".[191]

3.4.1.3 Remedial obligations

Review and redress are also important elements of States positive obligations to uphold communication rights in an online environment. In accordance with Article 13, ECHR, States must, first and foremost, ensure that effective remedies are available for violations of communication rights. Remedies should have corrective, compensatory, investigative and punitive functions and effects. These obligations mean that States must ensure that alleged violations of communication rights by private parties are subject to independent and impartial judicial review.[192] Such review would necessarily consider the extent to which policies and practices of private actors, e.g., for blocking and filtering content, show due regard for process values such as transparency and accountability, as well as respect for rule of law.[193]

3.4.1.4 General guidance

Primary guidance for ongoing attempts to clarify the scope and content of States' positive obligations to guarantee the effective exercise of communication rights in an online environment is provided by the ECHR, as interpreted by the ECtHR. In that context, the ECtHR has stated that the legitimate aims of restrictions on, for example, the rights to privacy and freedom of expression (as set out in Articles 8(2) and 10(2)) may be relevant for assessing whether States have failed to honour relevant positive obligations.[194] The ECtHR has also found that the margin of appreciation is, in principle, the same for Articles 8 and 10, ECHR.[195] In all cases involving competing rights guaranteed by the Convention, a fair

[188] *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* [GC], no. 45036/98, ECHR 2005-VI; *M.S.S. v. Belgium and Greece* [GC], no. 30696/09, ECHR 2011.
[189] *Informationsverein Lentia, op. cit., VgT, op. cit., Manole & Others v. Moldova, op. cit.*
[190] *Dink v. Turkey, op. cit.*
[191] E. Montero and Q. Van Enis, "Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: Squaring the circle", *op. cit.*, at 24.
[192] See also in this connection, Council of Europe Commissioner for Human Rights, Recommendation 16 (2014).
[193] See, e.g., *Peck v. the United Kingdom, op. cit.*
[194] *Rees v. the United Kingdom*, 17 October 1986, Series A no. 106, *Von Hannover 2, op. cit.*
[195] *Von Hannover 2, op. cit.*, para. 106.

balance has to be struck between the rights involved, as relevant for the particular circumstances of the case. However, when restrictions are imposed on a right or freedom guaranteed by the ECHR, in order to protect "rights and freedoms" which are not guaranteed by the ECHR, the ECtHR has insisted that "only indisputable imperatives can justify interference with enjoyment of a Convention right".[196]

The CJEU generally takes a similar "fair balance" approach to that of the ECtHR and has arguably gone so far as to extend the need for private parties to strike a fair balance between competing fundamental rights whenever their activities or omissions interfere with those rights.[197]

3.4.1.5 Specific guidance

In their case-law, the ECtHR and the CJEU tend to give guidance of a general nature to States about the nature and scope of their positive obligations. Specific guidance, therefore, usually has to be sought elsewhere or inferred from other sources, for instance Declarations and Recommendations adopted by the Committee of Ministers of the Council of Europe and Directives adopted by the European Union. Although such sources of specific guidance are typically policy or political texts and are therefore not legally-binding on States, their influence can be persuasive. They can explore the ramifications of principles beyond the immediate context of the given set of factual circumstances in which the principles have been identified.

Specific guidance can also be gleaned from ongoing efforts at the global level to sensitize corporate entities to their human rights responsibilities and the relationship between traditional legal *obligations* of States and those corporate *responsibilities*. Although (the practical impact or effectiveness of) such initiatives are sometimes met with scepticism, their relevance stems from the architecture of international law that generally creates formal legal obligations for States, but not for private (corporate) entities.

3.4.2. The United Nations framework

In recent years, a campaign to strengthen corporate respect for human rights has achieved considerable traction within the United Nations system. It has generated a powerful political dynamic, even if it has not (yet) led to new legally-binding standards. A selection of key reference points in the campaign will now be sketched, in particular the UN Global Compact and the UN "Protect, Respect and Remedy" Framework for Business and Human Rights. These initiatives and their implementation are making steady inroads into European-level policy-making on relevant issues.[198] The Global Network Initiative (GNI), which has a more specific focus on information and communications technologies (ICT), will then briefly be reviewed as well.

3.4.2.1 The UN Global Compact

[196] *Chassagnou and Others v. France* [GC], nos. 25088/94, 28331/95 and 28443/95, § 113, ECHR 1999-III.
[197] See the analysis of the *UPC Telekabel Wien* judgment, above.
[198] See, by way of recent example, European Parliament Resolution on the freedom of press and media in the world (June 2013).

The UN Global Compact styles itself as the world's largest corporate responsibility initiative. It is a voluntary initiative, based on CEO commitments to align business operations and strategies with ten principles which have been distilled from selected international instruments spanning the subject areas: human rights, labour, environment and anti-corruption.[199] The first two principles focus on human rights:

> Principle 1: Businesses should support and respect the protection of internationally proclaimed human rights; and
> Principle 2: make sure that they are not complicit in human rights abuses.

These two principles represented very important inclusions in the Compact when it was launched in 2000. Since then, while the importance of the principles has not diminished, their development and promotion have been increasingly assured by the "Protect, Respect and Remedy" Framework for Business and Human Rights.

3.4.2.2 UN "Protect, Respect and Remedy" Framework for Business and Human Rights

The Framework, loosely inspired by the "respect, protect, fulfil" approach, is set out (*inter alia*) in a very influential report written by Prof. John Ruggie in his capacity as (former) Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises. The Framework recognises that there are problematic "institutional misalignments in the business and human rights domain" (para. 7) and accordingly seeks to offer guidance on how to fill the normative gaps that result from those misalignments. It addresses "all social actors": "States, businesses, and civil society" and their need for a "common conceptual and policy framework" (para. 8).

The structure of the Framework is triangular: it comprises three complementary, mutually-supporting principles. Each of the principles is alluded to in its title: the state *duty* to *protect*; the corporate *responsibility* to *respect*, and access to remedies (emphasis added).

<u>State protection</u>

States' duty to protect human rights comprises four main prongs. First, governments should foster corporate cultures in which respecting rights is an integral part of business activity (para. 29). Second, States should enhance policy alignment when it comes to the implementation of their human rights obligations. In other words, they should enhance the (vertical) coherence of the implementation of the their obligations under international human rights law, and the (horizontal) coherence of the implementation of their obligations by coordinating cross-agency responsibility for the same (para. 33). The third prong concerns the international level and the guidance and support that treaty bodies and special procedures can give States on implementing their obligations to protect rights vis-à-vis corporate activities (para. 43). The fourth and final prong concerns special measures for conflict zones (paras. 47 *et seq*.).

<u>Corporate responsibility</u>

The notion of corporate responsibility to respect human rights is explored from four main angles: respecting rights, due diligence, sphere of influence and complicity.

[199] See: https://www.unglobalcompact.org/what-is-gc/mission.

- *Respecting rights*

The responsibility to respect human rights is the "baseline expectation for all companies in all situations", although companies may incur additional responsibilities, for example, when they perform certain public functions or have voluntarily entered into additional commitments (para. 24). The separateness but complementarity of corporate responsibility to respect human rights and States' duty to protect them is crucial:

> The corporate responsibility to respect exists independently of States' duties. Therefore, there is no need for the slippery distinction between "primary" State and "secondary" corporate obligations - which in any event would invite endless strategic gaming on the ground about who is responsible for what. [...][200]

- *Due diligence*

In order to respect human rights, companies must exercise due diligence, which entails, first, deriving benchmarks for their activities from key international human rights instruments. It also entails developing a due diligence process that should include: policies, impact assessments, integration [of human rights policies throughout a company], tracking performance. Due diligence therefore comprises substantive and procedural elements.

- *Sphere of influence*

The notion of sphere of influence looks at the impact of companies' activities and relationships on human rights beyond the workplace. The term "conflates two very different meanings of influence: one is impact, where the company's activities or relationships are causing human rights harm; the other is whatever leverage a company may have over actors that are causing harm." (para. 68). The latter only falls under the company's responsibility to respect in particular circumstances.

- *Complicity*

This notion refers to "indirect involvement by companies in human rights abuses - where the actual harm is committed by another party, including governments and non-State actors" (para. 73), eg. the facilitation of unlawful State surveillance of individuals by Internet service providers or telecommunications operators. Complicity is generally made up of two elements:

1. An act or omission (failure to act) by a company, or individual representing a company, that "helps" (facilitates, legitimizes, assists, encourages, etc.) another, in some way, to carry out a human rights abuse, and
2. The knowledge by the company that its act or omission could provide such help.

Furthermore, it can take different forms:

- **Direct complicity** — when a company provides goods or services that it knows will be used to carry out the abuse.

[200] (para. 55). See also para. 70. See further: The Importance of Voluntarism (2009): https://www.unglobalcompact.org/docs/about_the_gc/Voluntarism_Importance.pdf.

- **Beneficial complicity** — when a company benefits from human rights abuses even if it did not positively assist or cause them.
- **Silent complicity** — when the company is silent or inactive in the face of systematic or continuous human rights abuse. [...]

Access to remedies

"Effective grievance mechanisms" are identified as being of central importance in the context of both the State duty to protect human rights and the corporate responsibility to protect human rights. Again, the separateness and complementarity of State and corporate approaches is stressed and it is also posited that non-state mechanisms "can offer additional opportunities for recourse and redress" (para. 86). A number of different types of mechanisms are itemised, including: judicial, non-judicial; company-level and multi-stakeholder or industry initiatives and financiers.

Non-judicial grievance mechanisms should be, at a minimum: legitimate, accessible, predictable, equitable, rights-compatible and transparent (para. 92). The degree to which a non-judicial grievance mechanism adheres to these principles is one measure of its credibility and effectiveness. As such, these principles could have a useful benchmarking function.

They should include in-built safeguards to avoid conflicts of interest whenever the company is directly involved in administering a mechanism, eg. by focusing on direct or mediated dialogue, with oversight structures, etc. Crucially, the report insists that these mechanisms "should not negatively impact opportunities for complainants to seek recourse through State-based mechanisms, including the courts" (para. 95).

Such mechanisms could offer a range of different types of redress to aggrieved parties: compensation, restitution, guarantees of non-repetition, changes in relevant law and public apologies.

Synopsis

Much of the value of Ruggie's report lies in how it prises open the traditional parameters of international human rights law and clarifies the "interloper" position of private/corporate actors in that underexplored legal terrain. Moreover, the report does not limit itself to the identification and explanation of principles; it also makes considerable efforts to set out how those principles could be operationalised. The unpacking of key concepts is designed to advance the goal of operationalisation. The report contains the germ of subsequent documents (also developed under Ruggie's stewardship): *Guiding principles on business and human rights: Implementing the United Nations' "Protect, Respect and Remedy" Framework*; *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide*.

3.4.2.3 The UN Special Rapporteur on the right to freedom of opinion and expression

As of this writing, the UN Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression, David Kaye, had announced a new project "to study the responsibilities of the Information and Communication Technologies (ICT) sector to protect and promote freedom of expression in the digital age".[201] This project will examine, *inter alia*,

[201] See further: http://ohchr.org/EN/Issues/FreedomOpinion/Pages/Privatesectorinthedigitalage.aspx.

the relationship between corporate responsibilities of ICT companies and the right to freedom of expression. According to a call for submissions on the Special Rapporteur's website, the initial phase of the project will be a mapping exercise, which will be the focus of the Special Rapporteur's report to the UN Human Rights Council in June 2016. The call for submissions provides further information about the initial phase of the project as follows:

> During the initial phase of the project until the spring of 2016, the Special Rapporteur will prepare a study that maps 1) the categories of actors in the ICT sector whose activities implicate the freedom of opinion and expression; 2) the main legal issues raised for freedom of opinion and expression within the ICT sector; and 3) the conceptual and normative work already done to develop corporate responsibility and human rights frameworks in these spaces, including governmental, inter-governmental, civil society, corporate and multistakeholder efforts. This report will also identify the work plan and objectives for the duration of the project.[202]

3.4.3. Self-regulatory initiatives

3.4.3.1 Global Network Initiative (GNI)

The GNI is the most prominent global effort towards self-regulation in the ICT sector. It includes amongst its participants ICT-companies such as Facebook, Google, LinkedIn, Microsoft and Yahoo! Its other participants are from, inter alia, civil society and academia, such as Human Rights Watch and Harvard's Berkman Centre.[203] Founded in 2008, the GNI established a set of principles on privacy and freedom of expression, which were translated into more concrete policy recommendations in its Implementation Guidelines.[204] The Principles, which are based on international human rights standards, have as their key focuses: freedom of expression, privacy, responsible company decision-making, multi-stakeholder collaboration and governance, accountability and transparency.

GNI members are expected to report on their activities and to submit themselves to independent assessments of their compliance with GNI guidelines.[205] However, there are no sanctioning powers or other mechanisms in place to enforce such compliance.

The GNI has been subject to criticism for its inactivity, and its difficulty in attracting new commercial members.[206] The Electronic Frontier Foundation withdrew its membership in 2013 due to a breakdown in trust regarding their independence from government influence following the 2012 NSA surveillance revelations.[207] Recently, the GNI seems to have gained

---

[202] *Ibid.*
[203] For a complete overview of participants, see: https://globalnetworkinitiative.org/participants/index.php.
[204] See further: https://globalnetworkinitiative.org/corecommitments/index.php.
[205] See further: https://globalnetworkinitiative.org/sites/default/files/GNI_-_Governance_Accountability_Learning.pdf.
[206] See, for example: http://www.forbes.com/sites/larrydownes/2011/03/30/why-no-one-will-join-the-global-network-initiative/; http://www.huffingtonpost.com/2011/03/07/global-network-initiative_n_832408.html; http://www.nytimes.com/2011/03/07/technology/07rights.html.
[207] 'EFF Resigns from Global Network Initiative', Electronic Frontier Foundation Press release, 10 October 2013, available at: https://www.eff.org/press/releases/eff-resigns-global-network-initiative.

more relevance with Facebook joining in 2013,[208] and the publication of the GNI's first company assessment in 2014, which reviewed participating companies' observance of GNI principles on freedom of speech and privacy.[209] It found all three companies reviewed – Google, Microsoft and Yahoo! – to be in compliance. It is unclear what direct consequences a negative outcome would have had. Until the GNI manages to obtain some powers to impose sanctions for breaches of its principles or otherwise enforce its guidelines, the GNI can best be seen as a platform to create awareness and share best practices.

The above discussion shows that online commercial actors have been prepared to enter into self-regulatory regimes aimed at safeguarding end users' fundamental rights. These initiatives range from nationally-bound to global cooperation, and from sector-specific rules on social media services to principles aimed at governing the entire ICT industry. Generally, globally active industry leaders have stated their preference for worldwide guidelines, and have resisted country-specific collaboration. However, these projects have not yet resulted in binding, enforceable codes of conduct, which means that existing self-regulatory initiatives govern the activities of the online intermediaries described in the case studies in Part II of this study only to a limited extent. As explained in the Introduction to this study, the case studies are styled as instances of privatized enforcement measures that are particularized rather than sectoral. It is interesting to note that a number of the examples used in the case studies involve GNI members.

[208] For commentary, see: A. Kulikova, 'Facebook Joins the Global Network Initiative – What to think of it?, LSE Media Policy Project Blog, 24 May 2013, http://blogs.lse.ac.uk/mediapolicyproject/2013/05/24/facebook-joins-the-global-network-initiative-what-to-think-of-it/.

[209] GNI, *Public Report on the Independent Assessment Process for Google, Microsoft and Yahoo*, 8 January 2014, available at: https://globalnetworkinitiative.org//news/gni-report-finds-google-microsoft-and-yahoo-compliant-free-expression-and-privacy-principles.

PART II

4. Case studies of privatized enforcement measures

4.1.Context

4.1.1. Introduction

The second part of this study uses three case studies to consider the use of privatized enforcement measures by online intermediaries. It focuses on the qualitative differences between various techniques employed in blocking and filtering practices by online intermediaries. In examining these techniques, the study considers the extent to which certain methods currently used for privatized enforcement online are compatible with fundamental rights, most notably the right to freedom of expression, the right to access information, the right to privacy, data protection rights, the right to a fair trial, the right to an effective legal remedy, the freedom to conduct a business and the freedom to provide services.

The focuses of the case studies are:

- Non-judicial notice-and-takedown procedures of social networking services;
- Voluntary use of content-ID tools by hosting providers to avoid liability for illegal content, and
- Voluntary scanning of private data by online service providers and the subsequent reporting of users to law enforcement agencies.

As explained in Part I of this study, the European and international human rights framework is traditionally applied in the context of state-related measures. Yet, given that public and private communications are now largely intermediated by private actors, the role of the state is changing and may appear to be becoming more peripheral. The application of human rights in this domain requires further refinement to fully take account of these changes. In order to set the stage for the case studies, it is useful to first identify potential factors that are relevant to this assessment. Three potential factors will be considered here: degrees of dominance of online intermediaries, degrees of state involvement in self-regulatory or privatized enforcement measures and potential remedies for breaches of rights.

4.1.2. Degrees of dominance

An increasingly important theme in the analysis of the applicability of human rights to online self-regulation is the dominance of a company. In the context of competition law, dominance is generally related to a company being able to sustainably increase its prices or lower its quality. From the perspective of individual users, however, dominance is more usefully framed in terms of dependence. In situations of dependence, it is unattractive for users to switch to other companies, for example because there are few (or no) viable alternatives or because switching is costly.

In the online environment, highly concentrated markets are not uncommon. This is partly due to network effects: a service connecting its users becomes more attractive as its user base

grows. Alternatives are often unattractive because of their lack of users.

Even in the absence of market concentration, companies sometimes agree to coordinate their measures across a market. When those companies are dominant in a given market and there is dependence on their services, it can become impossible for a user not to be subject to those coordinated measures. An arguably positive example of such practice is the coordinated blacklisting of spam-sending IP-addresses.

In markets where the service facilitates transactions between customers and non-customers, the effects of concentration are further compounded. It can then be nearly impossible for a user to avoid interactions with a dominant company. For example, even if one does not have a Gmail-account oneself, it is difficult to avoid e-mailing Gmail-users.

The dependence on a certain service can also be related to the nature of the service. For example, services which mostly provide entertainment, could more easily be abandoned than services that are also used for more business purposes or for interacting with the government.

Thus, the degree of dominance of a company is relevant in three ways for a human rights analysis. Whenever a company has a broad customer base, measures applied by the company affect large numbers of people. In addition, where the company also facilitates interactions with non-customers, those measures also (indirectly) affect people who did not even choose to become a customer. Lastly, the nature of the service can make it more difficult to abandon a service, for example when the alternative services are very limited or are not of practical worth.

4.1.3. Degrees of state involvement

As pointed out in the Introduction, this study concerns "pure" self-regulation, as opposed to other forms of regulation, such as co-regulation. Even within this narrow field, however, various degrees of state involvement can be identified and distinguished. It is useful to provide a rough outline of these varying degrees as a precursor to the case studies.

At the one end of the spectrum, one can think of purely voluntary self-regulatory measures – without any involvement or pressure from the state or others whatsoever. Measures could, for example, be intended to safeguard the reputation of a company, to cater to specific religious convictions or to lower the operating costs of a company. Often, however, these measures are less voluntary than they may appear at first sight.

Firstly, the state can have a hand in the process of creating the measures. The state could facilitate meetings between companies to agree on coordinated measures, providing the meeting space, drafting the agenda and taking notes, etc. Even when the outcome of such meetings may be a completely private agreement, a certain degree of state involvement should be acknowledged (where it exists).

Secondly, the state can have a hand in influencing the substance of measures. The most obvious example would be where the state instructs companies to take measures and that the failure to do so will lead to the state introducing legislation with the same aim. The state could also be involved as a participant in coordinated discussions between industry players (which could also be considered a form of co-regulation). Alternatively, the state could offer

financial incentives to steer measures.

Lastly, the state can be involved in the execution of self-regulatory measures. For example, the government may inform service providers that certain information published on their platform violates their terms of service, without it being illegal. This is exactly what the Dutch government is doing in order to remove websites it deems undesirable, as research by Bits of Freedom has shown.[210]

The degree of state involvement is very relevant for the research question that this study sets out to answer. Traditionally, "state action" is required to trigger the application of the human rights framework. The above already suggests that too rigid an understanding of the "state action"-doctrine would not do justice to the varying degrees of, and degrees of complexity of, state involvement in self-regulatory measures.

In addition, a more detailed analysis of these kinds of state involvement should also be related to other factors, such as the degree of dominance discussed above. When a relatively "light" form of state involvement relates to a measure taken by a dominant party, this should arguably be more quickly considered as "state action", than when it relates to a measure taken by a small (i.e., non-dominant) party.

4.1.4. Potential remedies

Lastly, potential remedies to address infringements also differ. This particular subject is not thoroughly investigated in the present study and merits further research, so we only touch briefly on selected examples here.

One of the shortcomings often identified with self-regulatory measures is the lack of democratic legitimacy: the rules are decided by private parties without consultation with persons affected by the rules or a form of oversight by those persons, even though they have effects which in some cases are quite comparable to laws adopted by a parliamentary procedure. This shortcoming, where it is present, could be addressed by introducing certain due process obligations on the service provider, possibly by legislative means.

Another remedy, related to the first, would be the imposition of transparency obligations. The provider could, for example, be obliged to have unambiguous terms of service, and also apply them in a fair and non-arbitrary manner. This could also take the form of a requirement to report on the effectiveness of a certain measure, taking into account its stated goals. Both possibilities would fall under the banner of fundamental rights-driven consumer protection.

As a more far-reaching requirement, one could imagine the necessity, proportionality and subsidiarity requirements being imposed on self-regulatory regimes. Factors such as the measures, their stated goals and their effectiveness and the severity of the infringement could be taken into account in such an assessment.

For the purposes of this study, it is sufficient to note that there is a plausible relationship between the factors set out above and the potential remedies that can be contemplated. A light degree of state involvement would only necessitate lighter remedies, such as those relating to

210 See Bits of Freedom 13 October 2014, "NCTV vraagt wat gevorderd moet worden", to be found at https://www.bof.nl/2014/10/13/nctv-vraagt-wat-gevorderd-moet-worden/.

transparency. A heavier degree of state involvement would, on the other hand, require more far-reaching necessity and proportionality obligations.

4.1.5. Conclusion

In conclusion, it is argued that the application of the human rights framework to self-regulatory measures in the online environment requires an assessment of the interplay between different elements. One element which plays an important role in the assessment is the dominance of the private actors involved. Another is the degree of state involvement. A third element is the remedies to address infringements. Other elements may also be identified, as will be seen in the case studies, below.

4.2.Case study 1: Social networking services

With the advent of web 2.0, the Internet has been transformed from a top-down repository of editorial content to a horizontal platform where all users can contribute. The introduction of comment sections, and the increasing ease and availability of free blogging and hosting services, are examples of web 2.0 methods of end-user participation. Increasingly, online services function as intermediary platforms for user-generated content. Although intermediaries typically do not exercise far-reaching control over transmitted content, they are nevertheless equipped with the means to remove communications and block users from their services. As such, these actors can occupy an influential position as 'gatekeepers' to online forms of expression.[211]

One category of user-generated content intermediaries which hold a place of particular importance in online discourse is Social Network Services (SNSs), more commonly known as 'social media'. Most definitions of this term include the following characteristics: SNSs allow for the creation of users profiles, enable customers to establish a network of connections to other users (displayed in connection lists), and to share content and communications within these networks.[212] The term may thus apply to a variety of intermediaries, such as blogging sites, wikis, chat services and discussion boards, all of which facilitate the creation of virtual communities.[213] Insofar as these platforms allow a broader range of users to voice their opinions and have them heard, SNSs have been hailed by some as contributing to the 'democratisation' of the media environment by lowering the barrier for civil society participation.[214]

The central role that SNSs have come to play in public debate requires a close examination of their observance of users' free speech rights. Many acts of civil society participation now originate in social networks, ranging from awareness-raising campaigns such as Kony2012 and the ALS Ice Bucket Challenge, to the organisation of public manifestations such as the Occupy movement, the spontaneous vigils following the *Charlie Hebdo* attacks and the #blacklivesmatters protests. They have even been important enabling factors for political revolt in the 2009 Iran uprising – often called 'the Twitter revolution'- and the Arab Spring revolutions.[215] Conversely, it has become difficult to imagine a significant social movement without a substantial social media presence. The Council of Europe has described online social networking services as "human rights enablers and catalysts for democracy".[216] Therefore, incidents such as Facebook's removal of the event page for an anti-Putin rally

[211] See further: J. Zittrain, 'A History of Online Gatekeeping', 19 Harv. J. Law Technol. 253 (2006); P.O. Looms, "Gatekeeping in Digital Media", Mapping Digital Media Reference Series No. 8, Open Society Media Program, April 2011.
[212] D. Trottier & C. Fuchs, 'Theorising Social Media, Politics and the State: An Introduction', in D. Trottier & C. Fuchs, Eds., *Theorising Social Media, Politics and the State* (Routledge, 2014); D. Boyd & N. Ellison, 'Social Network Sites: Definition, History and Scholarship', 13 *Journal of Computer-Mediated Communication* 1 (2008), p. 212-216.
[213] Trottier & Fuchs, *op. cit.*, p. 16-19.
[214] H. Margetts, 'The Internet and Democracy', in W. Dutton, Ed., *The Oxford Handbook of Internet Studies* (Oxford University Press, 2013).
[215] P. Howard & M. Huzzain, *Democracy's Fourth Wave?: digital media and the Arab Spring* (Oxford University Press, 2013).
[216] Rec CM/Rec (2012)4 of the Committee of Ministers to Member States on the protection of human rights with regard to social networking services.

should give us pause for thought.[217] Many social networks have created processes for the removal of user content without the need for a court-ordered injunction, but these systems can sometimes result in blocking measures which are questionable from a free speech perspective.

To what extent does this form of private ordering ensure the observance and enforcement of free speech rights? This case study will focus on two well-known SNSs, Facebook and Twitter, and examine their policies as to the voluntary removal of user content. It will start by examining the legal status of these platforms regarding their liability for hosted content under EU law, followed by a review of their opportunities and incentives for content censorship, including a discussion of their Terms of Service (ToS) and a critical examination of a selection of past blocking decisions.

4.2.1. The legal position of SNSs

Neither Facebook nor Twitter actively monitors its content in search of illegal or otherwise undesirable content. A Twitter spokesman has explained their blocking policy as follows: "The key is that this is **reactive only.** It's on a **case-by-case basis,** in response to a valid request from an authorized entity. […] Twitter does not mediate content, and we do not proactively monitor Tweets."[218] Facebook employs a similar policy, where content can be brought to the attention of a moderation team which does not independently seek out content for removal.[219] These SNSs thus take a passive, neutral approach towards the content their users generate, and blocking measures are reactions triggered by complaints from inside or outside their community.

This ostensibly neutral stance allows SNSs to qualify as 'hosting providers' under Article 14 of the E-Commerce Directive.[220] Consequently, they cannot be held liable for hosting content so long as they have no actual knowledge of its illegality and act expeditiously to remove it upon obtaining such knowledge.[221] Therefore, since SNSs can be expected not to perform any independent investigation of content legality, liability is only likely to arise once SNSs receive a notification by third parties which would provide them with such knowledge. Insofar as SNSs are willing to act on these notifications, the current legal framework thus provides tools for private parties to effectuate the removal of content from social networks without the need to obtain a court order.

It should be noted that notification alone does not automatically trigger a removal obligation for SNSs, as the CJEU has stated that liability only arises when the hosting provider 'was

---

[217] T. Parfitt, 'Russia blocks Facebook site urging rally for anti-Kremlin activist Alexei Navalny' *The Telegraph* 21 December 2014. http://www.telegraph.co.uk/news/worldnews/europe/russia/11306880/Russia-blocks-Facebook-site-urging-rally-for-anti-Kremlin-activist-Alexei-Navalny.html.

[218] A. Latifi, 'Making Sense of Twitter's Censorship', *Al Jazeera* 28 January 2012. http://www.aljazeera.com/news/americas/2012/01/201212835211882918.html.

[219] M. Sweney, 'Mums furious as Facebook removes breastfeeding photos', *The Guardian* 30 December 2008.

[220] Recital 42 E-Commerce Directive defines hosting acitvities as: '[activities] is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored'. See also Joined cases C-236/08 to C-238/08, *Google v. LVHM*, 23 March 2010 and Case C-324/09, *L'Oréal v. Ebay* (2011) I-06011, para. 112.

[221] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Article 14(1).

actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality'.[222] While illegality may be obvious in some cases, such as pre-teen child pornography, there are many examples where information is not so readily identifiable as such, including complex defamation disputes or politically controversial forms of hate speech. In such cases, the illegality of content is closely linked to the end user's free speech interests. A contribution to a public debate, may, for example, provide a defence against allegations of libel, while journalists may report on hate speech by others as a matter of public interest.[223] It therefore follows that, when faced with a notification of illegal content, SNSs are expected to make an independent assessment of the content's status. The determination of illegality by SNSs in such cases is thus inherently affected by the level of free speech protection afforded to end users. The CJEU's decisions in *Promusicae* and *UPC Telekabel* require them to strike a fair balance between the fundamental rights affected, including free speech, when implementing blocking injunctions, but it remains unclear whether they have such an obligation when deciding on voluntary removal and informal takedown notices.[224]

The above shows that the protection of end users' free speech rights will largely depend on their SNSs' evaluation of the competing rights involved. Where the often complex task of determining the legality of content would traditionally lie with the courts, the private ordering of online content requires SNSs to perform a similar examination. How can we expect them to perform this task? On the one hand, if SNSs are overly complacent with removal demands, this could lead them to block content where they have no legal obligation to do so. On the other hand, a more intractable approach might expose them to liability once judicial redress is sought, for failing to comply with their obligation of "expeditious removal". This raises the question of which of these two evils our social networks are more likely to choose.

4.2.2. Terms of Service and the assessment of takedown requests

There are numerous factors that make the protection of free speech rights in the face of takedown demands an unlikely prospect. First of all, it should be noted that SNSs generally include very broad blocking discretions in their Terms of Service (ToS), the contractual provisions which govern their relationship with end users. This can be illustrated by a brief review of Facebook and Twitter's content removal powers.

Article 5 of the Facebook ToS, titled 'Protection of Other People's Rights', starts with the following paragraphs:

(1) You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
(2) We can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies.[225]

Removal is thus permitted for those content categories prohibited under the Terms of Service, and for any content that infringes individual rights or violates the law. The contractual

[222] Case C-324/09 *L'Oréal and Others*, *op. cit.*, para. 122.
[223] See, for example, *Jersild v. Denmark*, 23 September 1994, Series A no. 298.
[224] See section 1, above.
[225] Facebook Terms of Service. https://www.facebook.com/legal/terms.

prohibitions are mainly outlined in Article 3, 'Safety'.[226] Its proscriptions range from rules on security, intellectual property and commercial usage to prohibitions of bullying, harassment and intimidation, as well as the posting of hate speech, pornography, nudity, and gratuitous violence. Article 3(10) even prohibits all use of Facebook "to do anything unlawful, misleading, malicious or discriminatory".[227] With such terms, there remains little which would not be susceptible for removal; exaggerated headlines, insincere compliments, retouched photographs, even misconstrued sarcasm could be considered misleading. What's more, these prohibitions apply to all cases where Facebook *believes* that a violation of their statement has occurred, which would relieve them of the burden of even having to prove the infringing nature of the targeted content. Thus, while content removal is conditional upon some form of contractual infringement or illegality, the contractual prohibitions are defined so broadly as to provide a large degree of interpretive discretion for Facebook, and end users are left with no meaningful contractual grounds to contest their blocking decisions.

A similar rule is in place for the termination of services to particular users, also known as 'banning', which could be considered an even more severe intervention measure. Article 12 of the Facebook ToS reads: "If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you."[228] Given the broad range of ToS prohibitions, as well as the prohibition of violations *in spirit*, users are once more faced with an almost unlimited removal discretion.

Whilst Facebook requires at least some infringement or illegality to permit termination and content removal, Twitter's powers of intervention are unconditional. Article 8 of the Twitter ToS reads: "(…) We reserve the right *at all times* (but will not have an obligation) to remove or refuse to distribute *any Content* on the Services, to suspend or terminate users, and to reclaim usernames without liability to you."[229] (emphasis added). Reference is made to 'the Twitter Rules', which outline Twitter's policy as to prohibited content.[230] In comparison to Facebook's content rules, they seem more protective of the user: besides rules on security and commercial communications, all they prohibit is impersonation, violent threats, 'unlawful use', and pornography. Nevertheless, these rules are merely guidelines within a contractual framework which allows any and all removals and bans.

This brief review shows that blocking measures will only result in a breach of contract under exceptional circumstances, since ToS provisions are so broad as to provide a pretext for removal for almost every takedown request imaginable. Furthermore, even if such a breach of contract were to occur, it is unlikely that the prospect of judicial redress by end users could go far in dissuading SNSs. Firstly, since SNSs are as a rule free-to-use services, and tend to prohibit direct commercial use of their networks, it is unclear which damages could result from blocking content – it is certainly unlikely to exceed the potential liability following from neglecting to remove, say, IP infringements or defamation. Secondly, most consumers are simply not likely to resort to judicial remedies in the first place – a phenomenon described by Lilian Edwards as the "inertia of consumers in relation to litigation".[231] These factors

[226] Facebook Terms of Service. https://www.facebook.com/legal/terms.
[227] Facebook Terms of Service. https://www.facebook.com/legal/terms.
[228] Facebook Terms of Service. https://www.facebook.com/legal/terms.
[229] Twitter Terms of Service. https://twitter.com/tos.
[230] The 'Twitter Rules': https://support.twitter.com/articles/18311-the-twitter-rules.
[231] L. Edwards, *WIPO Report: Role and responsibility of internet intermediaries in the field of copyright and related rights* (WIPO 2005), p.12, available at: http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf.

combined effectively prevent end users from playing an active role in correcting undue blocking decisions, which in turn might encourage intermediaries to pursue risk-avoidant content policies to the detriment of free speech.

It could be argued that end users have knowingly and willingly submitted themselves to the possibility of intermediary content moderation, as evidenced by their acceptance of the Terms of Use. The principle of consumer choice would then be invoked to justify the current framework for content removal. However, as Ellen Wauters, Eva Lievens and Peggy Valcke have pointed out, SNSs display many characteristics which limit the role of consumer choice in ensuring an appropriate level of protection.[232] These factors include the informational asymmetry between business and consumer, the network effects of social media and the investment required of users in establishing their profiles and networks (the 'stickiness' of social media).[233] In light of these considerations, unwarranted or unexpected content blocking should be not be seen as a possibility that end users knowingly and willingly subject themselves to as a result of free and informed choice between various online service providers. End users may be not be fully aware of removal conditions, or may simply lack suitable alternative options. Indeed, Facebook allows access to a potential audience of over a billion users worldwide, while Twitter counts over 250 million users. In terms of scope and reach, there are no equivalent alternatives for consumers unsatisfied with their broad removal competences. Considering the strong network effects of social media services, individual users have little meaningful choice in selecting their platform on the basis of free speech concerns, and are effectively forced into this environment of unrestricted and unforeseeable intermediary blocking powers.

The permissive terms described above stand in stark contrast to the principles and guidelines drafted by the GNI, of which both Facebook and Twitter are members. As regards freedom of expression, these include a subsidiarity principle ("Interpret government restrictions and demands so as to minimize the negative effect on freedom of expression" [234]) and transparency requirements towards affected end users. These recommendations provide a commendable ideal for SNS policies, and would go some way in protecting end users against arbitrary and unaccountable content removal. However, they are not yet reflected in the Terms of Service provided towards end users, who have no meaningful contractual grounds to hold SNSs accountable.

4.2.3. Blocking decisions in practice

A review of Facebook's past blocking decisions shows that many are necessary to comply with local laws and norms. On its website, it states that: "Holocaust denial is illegal in

[232] E. Wauters *et al.*, 'Towards a better protection of social media users: a legal perspective on the terms of use of social networking sites', *Int J Law Info Tech* (2014).
[233] Chiu defines the 'stickiness' of social networks as inviting "*repetitive visits to and use of a preferred Web site because of a deeply held commitment to reuse the Web site consistently in the future, despite situational influences and marketing efforts that have the potential to cause switching behavior*." T. Chiu, "Note. Irrationally bound: Terms of Use licenses and the breakdown of consumer rationality in the market for social network sites" (2011) *21 S. Cal. Interdisc. L.J.* 167-213, 10. On consumer consent in social media Terms of Use, see: E. Wauters *et al.*, 'Towards a better protection of social media users: a legal perspective on the terms of use of social networking sites', *op.cit.*
[234] Global Network Initiative, Implementation Guidelines, available at: https://globalnetworkinitiative.org/implementationguidelines/index.php.

Germany, and so if it is reported to us we will restrict this content for people in Germany".[235] While this particular national law could be considered a legitimate restriction of free speech, this country-specific approach has also led to some arguably un-democratic blocking measures. It would fall outside the scope of this study to address the jurisdictional complexities involved in the legal assessment of these cases, but these incidents can serve to illustrate the pressures on SNSs to censor their networks. For example, it has been reported that a number of Facebook pages dedicated to criticism of the dominant Hong Kong political party were banned without giving any reason in 2010.[236] Furthermore, a page aimed at organising a political rally organised by the prominent activist Alexander Navalney was also removed without a court order.[237]

Facebook has been criticised for removing numerous UK anti-monarchist activist pages in the run-up to the 2011 royal wedding.[238] The removal of these pages coincided with the arrest of numerous activists, although Facebook denied any link between these occurrences, and claimed that the removal was part of a routine, a-political removal of pages created under fake personal profiles (a violation of the ToS).[239] Even if we assume that Facebook was not acting under any outside pressure, and that this was a matter of mere coincidence (although, given the Russian cases this possibility cannot be ruled out for future incidents), this example illustrates how the broad range of prohibitions under SNS user agreements, coupled with far-reaching sanctions such as outright removal of entire pages, can potentially be used by governments to undermine legitimate, legal forms of expression.

Another interesting example was Facebook's refusal to remove a Mexican beheading video, based on their policy that displays of violence were to be prohibited only insofar as the content "encouraged or celebrated" these actions.[240] However, after extensive criticism in the UK, including comments from the Prime Minister, they altered their policy and decided to remove the video for being contrary to their prohibition of "gratuitous violence".[241] Here we see that, even absent explicit orders, government pressure can have far-reaching influence on intermediary content policies. Since there is no demonstrable causal link between David Cameron's statements and Facebook's policy changes, it would be difficult for end users to contest this blocking decision as a direct government restriction of their rights. In some cases this political pressure may not even be made in public settings, such as when Angela Merkel confronted Mark Zuckerberg over anti-immigrant hate speech on Facebook during a UN summit.[242] This private, off-the-record conversation only became known because a nearby microphone had accidentally been left on. In such cases of informal pressure it can be particularly difficult to demonstrate government involvement in what can amount to measures of censorship. As Yochai Benkler has argued, this "regulation by raised eyebrow"

---

[235] https://govtrequests.facebook.com/
[236] E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs, 2012).
[237] Parfitt, *op. cit.*
[238] J. Preston, 'Facebook Deactivates Protest Pages in Britain', *The New York Times Blog* 29 April 2011, available at: http://mediadecoder.blogs.nytimes.com/2011/04/29/facebook-deactivates-protest-pages-in-britain/?partner=rss&emc=rss.
[239] S. Malik, 'Activists claim purge of Facebook pages', *The Guardian* 29 April 2011, available at: http://www.theguardian.com/uk/2011/apr/29/facebook-activist-pages-purged.
[240] H. Siddique, 'Facebook Removes Mexican Beheading Video', *The Guardian* 23 October 2013, available at: http://www.theguardian.com/technology/2013/oct/23/facebook-removes-beheading-video.
[241] Siddique, *op. cit.*
[242] P. Donahue, 'Merkel Confronts Facebook's Zuckerberg Over Policing Hate Posts', *Bloomberg* 26 September 2015, available at: http://www.bloomberg.com/news/articles/2015-09-26/merkel-confronts-facebook-s-zuckerberg-over-policing-hate-posts.

allows states to circumvent free speech safeguards by placing pressure on intermediaries.[243] SNSs' broad powers of removal in private relationships thus create a point of entry for unaccountable state interference with online speech.

The eagerness of governments to rely on the speech regulating powers of SNSs services has become particularly clear in the activities of police referral units such as the UK's Counter-Terrorism Internet Referral Unit (CTIRU). These centres monitor SNSs and refer supposedly terroristic content to the intermediary responsible. Their policy is not to explicitly order the removal of such content, but rather to notify the intermediary who must then independently determine whether it constitutes a breach of its Terms of Service.[244] In this manner, the CTIRU claims to have achieved over 50,000 instances of content removal.[245] The EU's counter-terrorism coordinator Gilles de Kerchove has recommended that other Member States launch similar operations.[246] Europol has also launched its own EU Internet Referral Unit, which aims, *inter alia*, to coordinate such national efforts.[247] Here, the same fundamental dynamic is at play as in the above examples with Cameron and Merkel, albeit on a much larger scale; systems of non-binding pressure are exerted by state authorities in order to influence the ostensibly voluntary policies of SNS. By emphasizing the SNS's discretion rather than that of public officials, and by the standards of Terms of Service rather than the standards of the law, this "regulation by raised eyebrow" can be achieved without triggering conventional constitutional safeguards.[248]

Social media content moderation can also prove a threat to less overtly political forms of speech. For instance, an Italian woman's Facebook post showing of two women kissing in support of LGBT rights was removed as a violation of the prohibition on 'pornography and sexual content', after other users reported flagged this content for removal.[249] A similar source of controversy has been Facebook's policy to comply with requests for the removal of images of breastfeeding, due to the nudity involved.[250] These incidents show that non-judicial notification and takedown procedures do not have the sole function of avoiding liability for illegal content, but can also serve as a means for the SNS operator to employ more editorial

---

[243] Y. Benkler, 'A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate', 46 *Harv. C.R.-C.L. Rev.* 311 (2011).

[244] DS 1035/15, EU Counter-terrorism Coordinator input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015, Council of the European Union 17 January 2015, see: http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf.

[245] Hansard, HC Deb, 2 April 2014, c957, 2014-04-02, available online at: http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140402/debtext/140402-0003.htm#140402-0003.htm_spnew12.

DS 1035/15, EU Counter-terrorism Coordinator input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015, Council of the European Union 17 January 2015, see: http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf.

T. May, Home Secretary's Speech on Counter-Terrorism, *Gov.UK* 24 November 2014, available online at: https://www.gov.uk/government/speeches/home-secretary-theresa-may-on-counter-terrorism.

[246] DS 1035/15, EU Counter-terrorism Coordinator input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015, Council of the European Union 17 January 2015, see: http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf

[247] See further: http://data.consilium.europa.eu/doc/document/ST-7266-2015-INIT/en/pdf.

[248] P. Leerssen, 'Cut out by the Middle Man: The Free Speech Implications of Social Media Blocking and Banning in the EU', (2015) *JIPITEC* 6(2), 99-119.

[249] A. Withnall, 'Facebook suspends Italian woman's account after she posts image of two women kissing in support of LGBT rights' *The Independent*, 19 May, 2014, available at: http://www.independent.co.uk/news/world/europe/facebook-suspends-italian-womans-account-after-she-postsimage-of-two-women-kissing-in-support-of-lgbt-rights-9398750.html

[250] Sweney, *op. cit.*

forms of content curation.[251] In reference to the breastfeeding controversy, a Facebook spokesman has stated that "[t]he photos we act upon are almost exclusively brought to our attention by other users who complain."[252] However, the selective or inconsistent application of ToS prohibitions in these user-initiated content flagging processes allows Facebook to selectively intervene and remove content which it – or its user community – finds undesirable. This introduces an element of arbitrariness and intermediary interference which could be seen as detrimental to free expression and the media pluralism.[253] Furthermore, depending on how freely and proactively such intervention is performed by SNSs, these policies may raise questions as to their neutral character as intermediaries and thus their eligibility for protection under the safe harbour of Article 14 of the E-Commerce Directive.

Like Facebook, Twitter responds to removal requests by governments and third parties. On the whole, Twitter policy grounds for content removal are more restricted, so that far-reaching curation of otherwise legal content, such as Facebook's anti-breastfeeding decisions, has not yet occurred. Government requests have led Twitter to remove a group of national-socialist accounts in order to comply with German hate speech laws.[254] Other examples include the blocking of two accounts belonging to political dissidents in Turkey.[255] It has also resulted in compliance with Pakistani court orders to remove blasphemous content and in the blocking of a Ukrainian activist account at the request of a Russian court.[256] As the Electronic Frontier Foundation has argued, these decisions were remarkable in light of the fact that Twitter held no assets in these jurisdictions, and thus could not be compelled to comply with these orders.[257] Furthermore, the Russian order was aimed at a non-Russian account, which illustrates how, given the international span of SNS activity, (over)compliance with national rulings can also erode the effective enjoyment of free speech rights in other jurisdictions.

In a departure from its otherwise largely passive stance, Twitter has taken major steps to remove terrorist activity from its service. In 2015, Twitter tripled the size of its content moderation team, expanded their definition of prohibited 'violent or threatening' behaviour, and began experimentation with automated algorithms for the filtering of abusive or inappropriate content.[258] This policy shift and the resulting removals were not ordered by any court, but can instead be seen as a response to the demands of Twitter users, who might be offended or shocked by such content; to public opinion, in order to avoid a reputation of facilitating terrorism; and to demands of government authorities, who might otherwise resort to more coercive, intrusive measures.

---

[251] Leerssen, *op. cit.*
[252] Sweney, *op. cit.*
[253] The Report of the High Level Group on Media Freedom and Pluralism emphasised the increased importance of digital intermediaries such as search engines and social networks as access points to the internet and the important role they play in ensuring media pluralism.
See: Freiberga, V. et. al., A free and pluralistic media to sustain European democracy: Report of the High Level Group on Media Freedom and Pluralism, 21 January 2013.
http://ec.europa.eu/information_society/media_taskforce/doc/pluralism/hlg/hlg_final_report.pdf
[254] K. Connolly, 'Twitter blocks neo-Nazi account in Germany' *The Guardian* 18 October 2012, available at: http://www.theguardian.com/technology/2012/oct/18/twitter-block-neo-nazi-account.
[255] 'Twitter sperrt regierungsfeindliche Konten', *Frankfurter Allgemeine Zeitung* 20 April 2014, available at: http://m.faz.net/aktuell/politik/tuerkei-twitter-sperrt-regierungsfeindliche-konten-12903503.html.
[256] E. Galperin, 'Twitter Steps Down From the Free Speech Party', *Electronic Frontier Foundation* 21 May 2014, available at: https://www.eff.org/deeplinks/2014/05/twitter-steps-down-free-speech-party.
[257] Galperin, *op. cit.*
[258] Leerssen, *op. cit.*

A relatively recent innovation in Twitter's content moderation policy has been the application of 'content withholding' measures rather than outright blocking.[259] This entails that certain content which runs afoul of regional prohibitions such as territorial IP rights or national hate speech laws can be rendered inaccessible in those regions, without affecting regular use in other jurisdictions. While some have criticised this approach as a concession to the demands of undemocratic foreign regimes, it can also be seen as the lesser of two evils in comparison to the blocking of content on a global level.[260] If we return to the requirement from *UPC Telekabel* that a 'fair balance' of fundamental rights must not unnecessarily deprive internet users of lawful access to information, content-withholding could be seen as generally less restrictive than absolute blocking measures.[261]

That being said, the chilling effect that regional withholding measures have on online expression in foreign jurisdictions could also serve to stifle or disincentivize online forms of speech. The utility of social media for, say, Turkish dissidents or Ukrainian activists will be greatly reduced if these groups are incapable of reaching their local audience. While access to their content would remain possible for foreign users, the chilling effect of these region-specific measures could then still be detrimental to social media expression on a global scale. Therefore, while content-withholding might be seen as the 'lesser of two evils' in comparison to total removal, intermediaries must still apply these measures with restraint and be aware of their broader effects on online expression.

4.2.4. Conclusions

This case study indicates that the current legal environment does not adequately incentivize the observance and enforcement of free speech rights by Social Network Services *vis-à-vis* their users. Theoretically, free speech defences must be taken into account while assessing the legality of user-generated content, but the ECHR and EU fundamental rights frameworks have not yet confirmed an obligation on online intermediaries to uphold such a right in voluntary removal decisions (i.e., removal in the absence of an official injunction). Furthermore, the high transaction costs involved in this evaluation and the low level of user protection in ToS agreements make it so that SNSs rarely have a direct interest in upholding free speech. This may lead them to ignore or undervalue free speech arguments in assessing claims of illegality, or even to knowingly remove legal content without regard to their users' free speech rights. Thus, there are few legal mechanisms preventing social media services from becoming agents of arbitrary and unforeseeable censorship.

The lack of enforceable safeguards for end users provides a point of entry for state authorities, who can persuade SNSs to block content through informal pressure. This "regulation by raised eyebrow" effectively allows them to sidestep free speech safeguards otherwise applicable to direct state interference, especially where their involvement remains invisible to the affected end users. Furthermore, as SNSs have increasingly shown themselves prepared to remove legal content at the behest of private notifications and to proactively monitor their communities for policy breaches, it also provides a point of entry for private actors to unduly limit the speech of others. So long as the free speech principles embraced in self-regulatory

[259] See: https://support.twitter.com/articles/20169222-country-withheld-content.
[260] C. Arthur, 'Twitter Faces Censorship Backlash', *The Guardian* 27 January 2012, available at: http://www.theguardian.com/technology/2012/jan/27/twitter-faces-censorship-backlash.
[261] Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, op. cit.*

projects are not translated into directly enforceable rights for end users, this lack of safeguards presents a structural risk of abuse by both public and private interests.

4.3.Case study 2: Hosting content generated by users

4.3.1. Background

In the Internet ecosystem, hosting providers play a key role: they supply the hosting services that users need in order to upload content they have generated (User Generated Content or UGC). While this content can take the most disparate forms – e.g. videos, images, texts, audios, animations, etc. – platforms that offer to store and to make UGC available to the public have become the backbone of what is nowadays known as Web 2.0.[262] Usually, hosting providers offer an ample package of services to users. In addition to the possibility to store, i.e., merely upload content to their servers, they offer assistance and sometimes a comprehensive infrastructure that renders UGC more appealing, easier to consult or to search, or better looking.

Significantly, hosting providers can offer services that allow users to generate revenue from associated advertising. This is a very important aspect, as advertising is one of the main sources of income for hosting providers – and a strong incentive that attracts users to the hosting service. However, all these activities that exceed the mere offer of hosting capacity, in particular advertising, can be seen by courts as non-neutral activities, i.e., activities that have the potential to disqualify hosting providers from the specific safe harbour created to exempt them from secondary liability. Examples of this type of safe harbour can be seen in the EU E-Commerce Directive, the US Digital Millennium Copyright Act (DMCA), and the Canadian Copyright Act.[263]

It is therefore extremely important for hosting providers to meet the conditions required in order to enjoy the liability exemption. Activities such as those mentioned above, and in particular the offer of advertisements related to the potentially infringing video, could be interpreted by courts as acts performed under the authority or control of the intermediary, a circumstance under which the liability exemption does not apply.[264]

As will be outlined in this case study, an alternative course of action for intermediaries is to enter into voluntary agreements with right-holders and users in order to limit their liability exposure. As will be shown, however, this way is not as balanced towards all the subjects involved (namely towards users) as the legislatively regulated one.

4.3.2. Case scenario: YouTube

[262] The expression Web 2.0 refers to websites and services which employ technologies that "allow users to interact and collaborate with each other in a social media dialogue as creators of user-generated content in a virtual community". Examples of Web 2.0 include social networking sites, blogs, wikis, folksonomies, video sharing sites, hosted services, Web applications, and mashups". See https://en.wikipedia.org/wiki/Web_2.0.
[263] See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 *on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* [E-Commerce Directive]. Similar provisions are present in 17 USC 512 (created by the Digital Millennium Copyright Act Pub. L. 105-304 in 1998) and in Sec. 31.1 of the Canadian Copyright Act 1985 as amended. Important to note that while the E-Commerce Directive applies to all *illegal content* the reported North American provisions are limited to copyright.
[264] Id.

In order to better illustrate the depicted situation, a real example can be used. YouTube, the video-sharing website created in 2005 by three PayPal employees and owned by Google since 2006, lends itself perfectly to the exercise. Almost all the videos uploaded on YouTube are provided by users, even though some content is provided directly by right-holders. Any Internet user can watch the videos without any authentication, but only registered users can upload them. As a general rule, the maximum length of videos is set at 15 minutes; This limitation is not related to technical issues but to specific policy considerations: When no time limit was imposed most videos exceeding 15 minutes were infringements of copyright specific to TV shows and movies.[265]

Videos can be watched on the YouTube website or embedded in different websites, in such a way that users of an embedding website can watch the video without having to be visibly redirected to the YouTube website. The video, nonetheless, is physically stored on YouTube servers and not on those of the embedding website. YouTube also implements a number of localized websites, that is to say perfect copies of the main website, but translated into the local language and, frequently, adapted to the local legal framework. YouTube usually redirects users automatically to the localized version of the website on the basis of the IP address. This explains why, for instance, users from a given country trying to watch a video sometimes see the message "Video not available in your country" while users from a different country (or spoofing their IP address) can still watch that same video.

4.3.3. Voluntary measures: the Content ID tool

In spite of the described efforts to limit the upload of videos infringing third parties' copyright, YouTube, together with its parent company Google, has increasingly been the object of attention of right-holders' claims. Right-holders' perception of YouTube's business model is perplexed at best, since most of the content, they claim, is uploaded by users without the authorization of copyright owners. On several occasions right-holders have reported that the number of infringing videos available is in the order of hundreds of thousands, which have led to claims for billions of dollars in damages.[266]

In addition to the delicate liability issue, Google's vast financial strength constitutes a strong incentive in this type of litigation, an aspect that increases both the number of cases filed and the amount of damages sought.[267] To prosecute individual users is a time-, resource-, and reputation-consuming activity and, particularly for cases of copyright infringement, the amount in damages that courts award to plaintiffs does not always justify the investment. This is true also in countries such as the US, where courts under certain circumstances can award statutory damages up to $150,000 per infringement.[268] While the punitive nature of these kinds of damages is certainly perceived by the convicted infringer, it does not represent a real compensation for right-holders, if compared to industry's claims that attribute losses of

265 See "Uploading videos longer than 15 minutes" at https://support.google.com/youtube/answer/4523193?rd=1 and "Your 15 minutes of fame" at "http://www.youtube.com/blog?entry=oorjVv_HDVs".
266 See e.g. Viacom International, Inc. v. YouTube, Inc., No. 07 Civ. 2103 (S.D.N.Y.), decided on June 23, 2010. Note that the decision was appealed, partially overturned and remanded for consideration to the District Court in 2012; in 2013 the District Court reissued summary judgment in favour of YouTube.
267 See T. Margoni & M. Perry, "Deep pockets, packets, and safe harbours", *Ohio State Law Journal*, Volume 74, Number 6, 2013, 1195 - 1216.
268 See 17 U.S. Code § 504.

billions of dollars to 'piracy'. Additionally, many content and media corporations have become aware of the controversial perception that an aggressive and litigious strategy against individuals triggers in the public opinion.

Conversely, to prosecute a big corporation allows copyright holders to try to recover damages in the amount that they claim and to have a realistic expectation that the defendant, if convicted, will be able to pay the entire amount. Furthermore, the public opinion perception of lawsuits between corporations is much more neutral, compared to the case of a corporation suing individual users.

In 2007, in order to further limit the amount of uploaded infringing content and consequently its exposure to copyright infringement lawsuits, YouTube implemented the Content ID tool, a voluntary system that the promoters hoped could seriously limit – or even eliminate – the possibility to upload content previously identified as infringing.

A brief description of the tool is necessary due to the complexity of the issue. Right-holders that meet certain criteria are eligible to file a request to YouTube to be admitted to the program. Once accepted into the program, right-holders can submit their copyrighted material (any sort of audio-visual material) to YouTube, which in turn will "scan" it and store the resulting ID in a database. YouTube quantifies estimates that over 25 million IDs are stored in its database.[269] When a user uploads a new video on YouTube, the video is automatically checked against the ID content in the database and if a match is found YouTube will contact the right-holder. However, unlike what would happen in a typical case of notice and take down, in this case YouTube (*rectius* Google) shows its deep understanding of Web 2.0 social and economic dynamics by offering right-holders the possibility to take any of the following actions:

- Mute the audio that matches their music;
- Block a whole video from being viewed;
- Monetize the video by running ads against it;
- Track the video viewership statistics.

Interestingly, any of these actions can be country-specific, in light of the IP address identification mentioned above. Accordingly, right-holders are able to segment the market and determine in which countries they want the content to be blocked, or monetized, and in which the statistics of the video need to be analysed. The actions can also be device-specific, meaning that right-holders can determine which action should apply depending on the type of device (desktop, mobile, e-reader, embedding system) used.[270]

However, as previously stated, not every right-holder can participate in this scheme. To be approved, users "must own exclusive rights to a substantial body of original material that is frequently uploaded by the YouTube user community", a status currently enjoyed by approximately five thousand "partners".[271] Under this condition, it seems clear that the Content ID scheme's main function is to accommodate the needs of major audio-visual and media groups, and not those of small or individual right-holders. The latter can – except in very special cases – rarely demonstrate ownership of rights "to a substantial body of original

269 See https://www.youtube.com/yt/press/statistics.html
270 See "How Content ID works" available at https://support.google.com/youtube/answer/2797370.
271 See https://www.youtube.com/yt/press/statistics.html.

material that is frequently uploaded".

Another critical element that emerged in the aftermath of the introduction of the new tool relates to the accuracy of the ID matching system. As Fred von Lohmann – at the time attorney with the Electronic Frontier Foundation (EFF[272]) – noted, the tool has been used by some of the groups admitted to the program to remove extremely large amounts of audio-visual content.[273] Many of these removals were clear fair use cases,[274] which led to the author employing the concept of "wholesale censorship" to describe the practice.[275] Other observers called this a "fair use massacre" and substantiated the accusation with a number of real cases.[276] The problem is recognized by a large cross-section of civil and academic society, and projects aiming to monitor the evolution of removal claims have blossomed.[277]

Indeed, the use of copyright protected material can be legitimate due to specific exceptions and limitations to exclusive rights and fair use/dealing claims. As seen in the first part of this study, the CJEU and the ECtHR have developed a consistent body of case law on the matter of identifying in the 'fair balance' of the fundamental rights involved the theoretical framework within which specific solutions should be framed.

It seems self-evident that, while a sophisticated algorithm can effectively and efficiently identify similarities in uploaded content (but see the results of an independent test of YouTube's Content ID in 2009 concluding that, while the system was "surprisingly resilient" in finding copyright violations in the audio tracks of videos, it often failed to detect useful meta-information, such as repeat infringers[278]), the correct evaluation of a specific legal situation in which competing fundamental rights have to be balanced can only be achieved following clearly defined and transparent procedures and guarantees. The intrinsic difficulty of this type of evaluation is recognized by the law, which created specific mechanisms intended to balance conflicting claims and to give the party whose content was removed for alleged copyright infringement a fair chance to react to the allegations. As was seen in Part I of this study, the protection of fundamental rights in the online environment include the availability of effective remedies when such rights are infringed, as well as the guarantees of fair trials for alleged infringers.[279]

---

272 "The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development"; see https://www.eff.org/about.

273 F. von Lohmann, Testing YouTube's Audio Content ID System, April 29 2009, available at https://www.eff.org/deeplinks/2009/04/testing-youtubes-aud.

274 The Web is full of incidents reporting content wrongly removed due to the automatic and unchecked matches produced by the Content ID system. A good illustration is present on one of the forums hosted by Google: https://productforums.google.com/forum/?hl=en#!category-topic/youtube/how-to-use-youtube-features/eSjKSGBrFMo

275 F. von Lohmann, Testing YouTube's Audio Content ID System, April 29 2009, available at https://www.eff.org/deeplinks/2009/04/testing-youtubes-aud.

276 See C. Mcsherby, The Fair Use Massacre Continues: Now Warner's Going After the Babies, March 12, 2009, available at https://www.eff.org/deeplinks/2009/03/fair-use-massacre-continues-now-warner-s-going-aft.

277 See generally the *Chilling Effects Clearinghouse*, a collaborative archive founded by several law school clinics in the US, http://chillingeffects.org/; specific to YouTube removals, and active until recently, the project "YouTomb" hosted by the MIT, http://archive.is/youtomb.mit.edu.

278 Electronic Frontier Foundation, "Testing YouTube's Audio Content ID System", 29 April 2009, available at: https://www.eff.org/deeplinks/2009/04/testing-youtubes-aud

279 See J. Urban & L. Quilter, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act", *Santa Clara Computer and High Technology Law Journal*, Vol. 22, p. 621, 2006; W. Seltzer, "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment", *Harvard Journal of Law & Technology*, Vol. 24, p. 171, 2010.

These legal frameworks include the previously cited E-Commerce Directive (EU), DMCA (US) and the recently reformed Canadian Copyright Act. Whereas these interventions are characterised by marked differences in approach – and are certainly not exempt from problematic aspects – they can be seen as the statutory recognition of the complexity required in finding a proper balance between conflicting fundamental rights in the online environment.[280]

The Content ID system, on the contrary, can be seen as a procedure which checks *ex-ante* newly uploaded content against large databases of works owned by right-holders in real time.[281] During this largely automated phase the possibility to develop an analysis to ascertain whether a specific use can be covered by fair use/dealing or other exceptions or limitations to copyright (ELC) is clearly absent, a situation that leads to numerous cases of "false positives".[282] If a match is found, the right-holder is informed and can decide what to do with the content: block it in a variety of ways, monetize it, or analyse viewership. It is only at this point that the right-holder has the possibility to determine whether the use of his content could have been fair.

However, it is clear that in the light of the sometimes hundreds or thousands of daily notifications received, right-holders are usually unable to analyse all cases with the required attention even at this stage (and this phase is often out-sourced to third parties). Furthermore, right-holders' "conflict of interest" is equally apparent when they have to determine whether the use made by others of their own work in the absence of their own authorization can constitute a legitimate use.

Users are left with two choices: the first one is to take no action, in which case the content that they uploaded remains in the condition chosen by the alleged right-holder (e.g., muted, blocked or "monetized"). Alternatively, the uploader of the blocked content can decide to take action and dispute the claim. If this happens, the right-holder can release the claim or confirm it, in which latter case the uploader will still be able to "appeal" a Content ID claim (only up to three times and only if possessing a verified account in good standing), and the right-holder at this point will only be able to release the claim, or to "take down" the audio or video. The latter option, also known as "copyright strike" leads to an immediate halt to the audiovisual content, and causes the account of the uploading user to enter a state of "bad standing", with limited features. If three "copyright strikes" are received, the account is terminated.

A final critical element relates to "contractual agreements" concluded by YouTube and right-holders, which eliminate the possibility for users to oppose a claim of copyright infringement filed through the Content ID scheme or even in the case of a formal notification. YouTube informs users about "Videos removed or blocked due to YouTube's contractual obligations" and explains that:

280 While the Canadian approach does somehow resemble the US one in terms of granularity, it is still too young to be properly evaluated. The system created by the E-Commerce directive leaves to Member States the possibility to establish take-down procedures, but this opportunity has not been taken by the large majority of Member States.

281 See: http://www.youtube.com/yt/press/statistics.html.

282 See for a recent example regarding the block of a video in which a renown legal scholar during an academic conference showed a few seconds of a protected content, see http://kluwercopyrightblog.com/2014/10/13/who-owns-the-world-cup-the-case-for-and-against-intellectual-property-rights-in-sports/. This represents a clear case of 'false positive' as confirmed by the fact that the right holder was very responsive in releasing the block.

> "YouTube enters into agreements with certain music copyright owners to allow use of their sound recordings and musical compositions. In exchange for this, some of these music copyright owners require us to handle videos containing their sound recordings and/or musical works in ways that differ from the usual processes on YouTube. Under these contracts, we may be required to remove specific videos from the site, block specific videos in certain territories, or **prevent specific videos from being reinstated after a counter notification**. **In some instances, this may mean the Content ID appeals and/or counter notification processes will not be available.** Your account will not be penalized at this time" (emphasis added).[283]

In other words, users will be denied the possibility to have their content reinstated on YouTube not only in case of filing a Content ID claim, but even when filing a DMCA or DMCA-like counter-notification under the conditions established by e.g. Sec. 17 USC 512(g) or by other similar national legislation.[284]

This is upheld by the terms that users accept when registering for the service. YouTube's Terms of Service (at least in the US version) state that:

> "If a counter-notice is received by the Copyright Agent, YouTube may send a copy of the counter-notice to the original complaining party informing that person that it may replace the removed Content or cease disabling it in 10 business days. Unless the copyright owner files an action seeking a court order against the Content provider, member or user, the removed Content **may be replaced**, or access to it restored, in 10 to 14 business days or more after receipt of the counter-notice, **at YouTube's sole discretion**" (emphasis added).[285]

From this brief analysis it is possible to conclude that if procedures such as those autonomously created and self-regulated (e.g., Content ID) or those regulated by legislative intervention (e.g., DMCA) are intended to balance the position of right-holders and users in their quest for either fast removal or fast reinstatement, then YouTube's voluntary agreements with right-holders severely limit one side of this important balance, namely the one leading to the protection of users and of their ability to express themselves on the Internet.

4.3.4. Considerations on the Content ID tool as a private measure intended to limit the uploading of infringing content

Proponents argue that the Content ID scheme operates as a privately drafted buffer inserted just before the more serious notice and take-down procedure in order to bring more balance and flexibility to a system where opposing positions are creating considerable shortcomings. However, from what could be observed, Content ID can be better conceptualised as an additional layer that safeguards the interests of right-holders and, indirectly, of intermediaries, without offering any corresponding enhancement to users' interests.

Qualifying right-holders will benefit from an automated *ex-ante* system that flags all matching content offering them the possibility to block, monetize, or monitor it, eventually

---

[283] See: http://www.youtube.com/t/terms?gl=US.

284 Namely that the counter-notice contains all the legally required elements and that the right-holder does not file an action seeking a court order to restrain the subscriber from engaging in infringing activity, within the established time frame; See 17 USC 512(g)(2)(C).

285 See: http://www.youtube.com/t/terms?gl=US.

discriminating geographically or by device. This constitutes a set of interesting, and definitively more flexible, opportunities for right-holders to exploit their works in ways that the standard notice-and-take-down procedures do not envisage. The benefits for YouTube are equally evident: a much higher likelihood that the content will remain on its servers. This not only reduces the removal of content from the service (up to 25 million unique items), which already represents quite a remarkable result, but also permits YouTube to receive additional revenue from the associated ads. The revenue of Content ID ads account for a considerable share of the overall monetized views on YouTube.[286]

Nevertheless, users – the third element of this equation – do not enjoy any additional benefit; on the contrary, the total number of removal claims is greatly increased, as it is now based on an automated, *ex-ante* verification tool that is simply not able to decipher the usually complex cases of legitimate uses. Similarly, the possibility for users to resist take-down requests is not equally empowered: while it is true that a simple dispute of a Content ID claim will not automatically start a legal proceeding, it is also true that the Content ID scheme is not alternative or preliminary to a standard notice-and-take-down procedure. Right-holders can decide to file a formal removal request at any time, including during a Content ID claim, and cause not only the immediate removal of the content but also to "copyright strike" the account of the user. Therefore, it is left to the discretion of right-holders to decide which way to proceed: a standard notice and take-down procedure, a Content ID claim, or both.

Therefore, users are substantially left with the same tool that they had before: either to leave the content down or react and try to have the content reinstated facing the risks and the costs of a possible lawsuit against a corporation. Moreover, it can be added to this already critical picture that under the conditions explained above (i.e., YouTube's voluntary agreements with right holders), users are deprived of their right to a Content ID appeal or to a counter-notification procedure. The resulting situation for individuals expressing their creativity and ideas on YouTube and similar platforms is alarming.

It should be stressed that the main function of copyright is to strike a delicate balance between the interests of authors and other right holders in the control and exploitation of their works on the one hand, and society's competing interest in the fundamental rights to freedom to impart and receive information, privacy, and communication rights on the other hand.[287]

Fair use/dealing and ELC are an integral part of the copyright system because they are the recognition in positive law of society's interest that individuals should be allowed to make certain unauthorised uses of copyrighted material.[288]

Private ordering tools, such as those concluded between intermediaries and right-holders,

286 YouTube's statistics speak of hundreds of millions of dollars for partners, which means that an even bigger share is retained by YouTube. Wikipedia, citing the same statistic page but accessed in 2013, reports that a third of all YouTube monetized views were connected to Content ID; see http://www.youtube.com/yt/press/statistics.html and the cited Wikipedia entry for YouTube.

287 See T. Dreier, 'Balancing Proprietary and Public Domain Interests: Inside or Outside of Proprietary Rights?', in R. Cooper Drefuss, D. Leenheer Zimmerman and H. First, *Expanding the Boundaries of Intellectual Property*, Oxford, Oxford University Press, 2001, pp. 295-316; P.B. Hugenholtz, "Copyright, Contract and Code: What Will Remain of the Public Domain?", *Brooklyn Journal of International Law* 2000/26, pp. 77-90.

288 L. Guibault, *Copyright Limitations and Contracts: An Analysis of the Contractual Overridability of Limitations on Copyright*, The Hague, London, Boston, Kluwer Law International 2002, Information Law Series No. 9.

safeguard the respective interests which are usually connected with the commercial exploitation of the works and of the platforms. These agreements are usually imposed on users who are not in a position to negotiate specific terms or conditions, but can only accept "take-it-or-leave-it" services that not only have become a standard medium of expression in the on-line lives of billions of people, but which also often lack realistic alternatives.

Individuals' communication rights are strikingly absent in the self-regulation model developed by intermediaries and right-holders. The resulting scenario is one where the legitimate uses linked to fundamental rights of the protected works, such as parody, critique, pastiche, news reporting, illustration for teaching, etc., are put under serious threat. The legitimacy of these kinds of agreements should accordingly be tested against the jurisprudence of the CJEU and ECtHR.

4.4. Case study 3: The scanning of private data and reporting users to law enforcement

Whereas the two previous case studies focused mostly on the communications freedoms aspects of measures imposed by private actors, this case study emphasises the privacy aspects. It takes as a starting point a highly topical issue: the voluntary scanning of private data by online service providers and the subsequent reporting of users to law enforcement agencies.

Several big online service providers have been found to engage in such practices. Firstly, in 2012 it was alleged that Microsoft automatically scanned privately accessible data in its cloud service OneDrive (formerly known as SkyDrive). Microsoft allegedly blocked the account of a Dutch user because he uploaded pornography, which was in violation of the terms of service of Microsoft, which at that time prohibited the storage of images containing nudity and partial nudity.[289]

The terms of service have since been adapted, and Microsoft now no longer prohibits the storage of nude pictures in its online drive service. The new terms do, however, provide that stored material is automatically scanned for images of sexual child abuse (but it does not say explicitly that users may be reported to law enforcement). Recently, a man was also arrested because he uploaded two images of sexual child abuse to his OneDrive account. Microsoft informed the US National Center for Missing and Exploited Children (NCMEC) when the two images were flagged by its systems, and the NCMEC got in touch with the Luzerne County District Attorney's Office.[290]

Google was in the news for a related activity: it automatically scans emails stored in Gmail for images of sexual child abuse. For example, it was reported that a 41-year old Houston man was arrested and charged with possessing child pornography after Google sent a tip to the NCMEC.[291] Microsoft's online email service Outlook also scans emails for sexual child abuse material.[292]

A third example of automated analysis of private data is Facebook. Facebook was in the news for analysing private chats on its platform and, together with other available data in the platform, reporting activity of possible predators to the police.[293] Reuters reported that "a man in his early thirties was chatting about sex with a 13-year-old South Florida girl and planned to meet her after middle-school classes the next day."[294] Using a self-developed algorithm for scanning postings and chats for criminal activity, Facebook automatically flagged the conversation, and employees then read the conversation and reported the man to the police. The police arrested him the next day.

---

[289] See http://www.forbes.com/sites/kellyclay/2012/07/19/is-microsoft-spying-on-skydrive-users/. Microsoft in its code of conduct for Windows services still prohibits using its services for depicting nudity, see http://windows.microsoft.com/en-us/windows-live/code-of-conduct .

[290] See http://www.philly.com/philly/news/Microsoft_cyber-tip_gets_Pa_man_arrested_on_child_pornography_charges.html

[291] See http://www.khou.com/story/news/crime/2014/07/30/houston-man-charged-with-child-porn-possession-after-google-cyber-tip/13378459/

[292] See https://www.microsoft.com/en-us/news/presskits/photodna/

[293] See http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712

[294] See http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712

It appears that this kind of scanning is currently primarily focused on sexual child abuse-related offences. Dropbox, however, is already reported to scan certain shared links to its online cloud storage platform and block copyright-infringing links.[295] It would not be surprising if broader copyright and terrorism-related scanning is already being considered – or even applied – as an interesting approach by certain stakeholders.

4.4.1. Scanning and reporting is an interference with privacy and sometimes communication freedoms

The scanning of personal data for these purposes is obviously an interference with the right to privacy. A user storing this data intends the data to be accessible only by him or her. The service provider, however, automatically scans the data and if it is flagged as suspicious, the data will be further analysed by employees. The company might then share information about the user with other organisations and law enforcement authorities.

The scanning is not only an interference with the privacy of users who are ultimately reported: it is an interference with the privacy of every user of the system, as the data of all users is subjected to analysis. This is particularly so for the scanning for matching images of sexual child abuse: all images stored in cloud or email services appear to be subjected to the matching software. The algorithm developed by Facebook to identify predatory behaviour appears on the other hand to have a certain proportionality built into the system: according to reports on the algorithm, Facebook does not monitor all chats, but only chats between minors and persons deemed to be potential predators, in view of attributes such as a high number of declined friend requests, a high proportion of contacts of one gender and the frequent changing of a birth date under and above the 18 years threshold.[296]

The fact that the scanning by the companies involved is partly automatic is not relevant for the question of whether this is an interference with the right to privacy: the application of automated scanning technology is also an interference with the right to privacy.

If the scanning is performed on private communications, it also amounts to an interference with communications freedoms, as the fear of surveillance can have a chilling effect for all users. Users will be less likely to use private chats or e-mail for the discussion of controversial matters, out of fear or uncertainty about potential consequences. This chilling effect is illustrated by a recent study on Google searches after the Snowden-revelations: it turns out that people use Google less often to search for terms which they deem controversial (such as 'porn' and 'tax avoidance').[297]

Lastly, the reporting to law enforcement is also an interference with privacy and, where applicable, communications freedoms. From a data protection perspective, the transfer of personal data to a third party is already considered a form of processing (which would thus be

[295] See http://techcrunch.com/2014/03/30/how-dropbox-knows-when-youre-sharing-copyrighted-stuff-without-actually-looking-at-your-stuff/

[296] See http://www.theguardian.com/technology/2010/apr/16/facebook-software-sexual-predators and http://www.forbes.com/sites/kashmirhill/2012/07/13/yes-facebook-scans-peoples-private-conversations-looking-for-sexual-predators-and-child-porn/.

[297] See A. Marthews and C. Tucker, *Government Surveillance and Internet Search Behavior*, 24 March 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564

subject to data protection rules). More particularly, being reported to the police because of a suspicion for these crimes obviously negatively affects the persons involved.

4.4.2. These are private initiatives with government links and very few serious alternatives

Goals. The explicit goals of these initiatives, namely the prevention and detection of sexual child abuse, are very important and universally recognised as such under relevant human rights frameworks. The distribution of images of sexual child abuse, in certain cases the possession of such images and sexual child abuse itself are also criminal offences, at least in the US and in Europe.

It must be noted that – notwithstanding the laudable goals of these programmes – their effectiveness is unclear, as little or no information on this is made publicly available. By extension, an analysis of the potential adverse consequences of such programmes, in particular the possible reduction of incentives for politicians to explore alternative, more effective methods to combat sexual child abuse, is lacking.

Interests. The measures used by companies appear at first sight to be taken not in the interests of the companies involved, but primarily in the interests of law enforcement. This could be concluded from the fact that scanning is directed at offensive behaviour taking place in private. Where, for example, Facebook has a very direct interest in ensuring that no unlawful and shocking material is made *publicly* available on its platform, it has a much more indirect interest in ensuring that no offensive behaviour takes place in the more private types of messaging on its platform, such as direct messages and messages shared only with friends (see further in this connection, Case study 1).

Upon further inspection, however, it becomes clear that companies have a vested interest in these kinds of programmes. Firstly, these programmes serve to bolster their reputation as "good citizens". Microsoft, for example, has dedicated part of its website to information on the development and licensing of its image matching software, called PhotoDNA, boasting how it has become the industry standard for combating images of sexual child abuse online.[298] In addition, these programmes arguably serve to politically legitimise the scanning of private data by these businesses for commercial purposes.

Government links. The image matching on cloud and mail services and Facebook's monitoring is by and large a private initiative. Microsoft, and others, such as Twitter and Facebook, use PhotoDNA. Facebook has been licensing Microsoft's technology since 2011, and Twitter has been using the technology since 2013.[299] The Facebook-monitoring algorithm appears to have been developed in-house by Facebook. There are no laws obliging these companies to perform this kind of scanning.

Certain links with government can also be identified, however. Firstly, from the news reports it can be gleaned that matches are used to tip off the National Center for Missing and Exploited Children (NCMEC), which subsequently reports to law enforcement. The NCMEC is authorized by US Congress to carry out a range of activities linked to the exploitation and

[298] See http://www.forbes.com/sites/kashmirhill/2014/08/05/the-tech-war-on-child-porn/
[299] See https://www.microsoft.com/en-us/news/presskits/photodna/ and http://www.theguardian.com/technology/2013/jul/22/twitter-photodna-child-abuse

abduction of children. These activities include the operation of a tipline to report internet-related child sexual exploitation and to transmit such reports to the appropriate local law enforcement agency for investigation.[300] It receives a small part of its funding from government sources, according to its 2012 annual report.[301] Secondly, a large part of the database on the basis of which images are matched is provided by law enforcement agencies. How the PhotoDNA database is generated is not completely clear, but it appears that part of its database is based on a set of images collected by Interpol.[302] In 2013, Google further reported that it was building a cross-industry database with part of the images provided law enforcement agencies and part by non-profits such as NCMEC and the Internet Watch Foundation.[303] In this respect, it is also important to note that the image database used by the companies consists of digital fingerprints (so-called hashes), which cannot be independently evaluated by the receiving companies to be indeed illegal – as the hashes cannot be reconstructed back into images. This means that the companies using the database are highly dependent on the providers of the digital fingerprints, such as the government. Thirdly, online service providers are arguably obliged to report suspected sexual child abuse when they become aware of the presence on their systems, although this provision explicitly imposes no obligation on these providers to monitor users pro-actively.[304] Fourthly, and most importantly, the scanning might ultimately result in government action: when one of the companies identifies an offender, law enforcement agencies will be informed, either directly or indirectly through NCMEC. These agencies subsequently might take action against offenders. Thus, through these initiatives, the government is arguably able to extend its surveillance powers – i.e., scanning the private data of users – to private communications and storage.

Safeguards. There is currently a lack of transparency with regard to the internally applicable procedures. The terms of service of Google, Facebook and Microsoft in theory allow for – and to a certain extent inform about – this kind of scanning, but neither of these provides detailed information on the practices themselves. It is unclear what kind of safeguards are implemented by these companies to prevent false positives. From the news reports discussed in the introduction to this case study, it appears that the suspect is not accorded any due process before handing the file over to law enforcement. This might have to do with the nature of the offence, which arguably requires an immediate governmental response, and informing the suspect would hinder the investigation.

Alternatives. The three services discussed above differ in terms of alternatives that are available. Email services are abundantly available, and there are many email services that do not use this kind of image matching technology. However, given the networked effects of e-mails, and given the size of Gmail and Microsoft's email services, it is very likely that you will have to communicate with people who will have their emails scanned by one of these companies. There are, consequently, very few serious alternatives to the e-mail services in question.

There are more alternatives to Facebook's private chat, although this is difficult to quantify. There are quite a few services available that allow for private chats outside of Facebook,

[300] See http://www.missingkids.com/Authorization
[301] See http://www.missingkids.com/en_US/publications/NC171.pdf
[302] See http://blogs.technet.com/b/publicyte/archive/2011/06/24/preventing-child-exploitation-microsoft-helps-create-photodna-digital-forensics-for-the-national-center-for-missing-amp-exploited-children.aspx
[303] See http://googleblog.blogspot.nl/2013/06/our-continued-commitment-to-combating.html
[304] See 18 U.S. Code § 2258A - Reporting requirements of electronic communication service providers and remote computing service providers, http://www.law.cornell.edu/uscode/text/18/2258A

including via Gmail and Ping. WhatsApp deserves special mention here, as it has been acquired by Facebook, but it is reported to implement end-to-end encryption in its chat application, thus obscuring private communications even to the service provider itself (which in this case is Facebook/WhatsApp).[305] As regards Facebook chat, it must be noted that Facebook is still a very popular platform and it can well be the case that for certain groups, it is difficult to avoid chatting via this social network. The issue described in the context of e-mail services, where the sender has no choice but to communicate via the e-mail provider of the recipient, does not apply, however.

Lastly, as regards alternatives to cloud services: there appear to be comparable services available which do not scan stored material, although not all of those services are free-of-charge.

4.4.3. Scanning and reporting, in particular of e-mail, problematic from a fundamental rights view

Given the above, it can be argued that the voluntary automated scanning for images of sexual child abuse, in particular of e-mail services, is problematic from a fundamental rights point of view. Not only are there strong links with government, mostly in the form of government provided databases of digital fingerprints, but the monitoring might ultimately lead to action by law enforcement. The government through these voluntary actions thus extends its strong arm and its surveillance powers. All companies are furthermore generally not transparent about these practices, merely suggesting that information can be monitored, and it is unclear whether internal procedures of due process are in place. And since the biggest e-mail providers in the world are performing such automated scanning, it is difficult to avoid being subject to this government-facilitated surveillance.

[305] See https://whispersystems.org/blog/whatsapp/.

5. Revisiting positive obligations of States

Having considered the three case studies of the use of privatized enforcement measures by online intermediaries, this is a relevant juncture to revisit the (positive) obligations of States and tease out the implications of those obligations in the context of privatized enforcement.

The following is a tabular overview of specific elements of States' positive obligations concerning privatized enforcement by online actors. These elements have been distilled from the above analysis of the case-law of the ECtHR and CJEU, as well as relevant standard-setting by the Council of Europe's Committee of Ministers. The focus is mainly on the rights to freedom of expression, privacy and data protection, (intellectual) property, an effective remedy and other procedural rights. This focus subsumes other rights mentioned earlier in Part I of this study, such as the rights to assembly and association, which are relevant for participatory rights in democratic society. The range of rights covered by this focus correspond to those typically implicated in the fair balancing of fundamental rights that informs the nature and scope of States' positive obligations. Indeed, the table as a whole should be read in the spirit of the need to strike a fair balance between fundamental rights, as consistently urged by both the ECtHR and the CJEU.

The first column describes the nature of the positive State obligation in general terms. The second column points to where the obligation is laid down. The third column explains the aims of the positive obligation. The final column, drawing in part on the three case studies, suggests specific implications of the more general obligation that are relevant for governing the activities of online intermediaries. It must be borne in mind that these are implications for the States themselves, i.e., indications of measures that States are obliged to take to ensure that fundamental rights are exercised effectively in the relations between online intermediaries and their users. They are not presented as actions to be taken by the intermediaries themselves, as such.

Positive obligation	**Source**	**Aims**	**Implications**
Guarantee (media) pluralism	*Informationsverein Lentia, Khurshid Mustafa & Tarzibachi, Appleby, Manole & Others*	Prevent monopoly or mitigate dominance of powerful groups/media	Ensure availability of viable expressive alternatives, bearing in mind different functionalities of different media. Ensure other fundamental rights (e.g., to property or to conduct a business) do not prevent effective exercise of right to freedom of expression or destroy its essence, esp. when private property has *de facto* public function.
Create a favourable environment for participation by everyone in public debate	*Dink, Yildirim, Steel & Morris, Khurshid Mustafa & Tarzibachi*	Prevent discriminatory access to media and forums of debate	Ensure measures restricting access to content, services or infrastructure are not discriminatory or overly broad, or cause collateral censorship.
Create a favourable environment for freedom of expression for everyone without	*Dink*	Prevent threats, violence and other crimes against participants in public debate and chilling effects arising from the same	Ensure effective legislative frameworks are in place to counter such offences. Ensure privacy of communications (data) and put in place safeguards

fear			against arbitrary surveillance.
Ensure effective procedural safeguards and effective remedies in respect of the right to freedom of expression	CM Recs, *UPC Telekabel*	Prevent arbitrary and non-transparent interference with right to freedom of expression without checks, balances and remedies	Ensure climate in which any interferences by online intermediaries with access to content, services or infrastructure are proportionate, transparent and subject to administrative and judicial review, with appropriate remedies being available.
Ensure effective procedural safeguards and effective remedies in respect of the rights to privacy and data protection	*Klaas, Kruslin, Malone, UPC Telekabel*	Prevent arbitrary and non-transparent interference with rights to privacy and (in particular) data protection without checks, balances and remedies	Ensure existence of regulatory framework and that it and its underlying principles are applied effectively in respect of online technologies. Ensure privacy of communications (data) and put in place safeguards against arbitrary surveillance. Ensure any interferences by intermediaries meet criteria of: legality; foreseeability; necessity; transparency; proportionality; effectiveness and reviewability. Provide for notification process by intermediaries whenever personal data is voluntarily passed on to law enforcement authorities or other parties.
Guarantee that intellectual property rights are fairly balanced against freedom of expression rights	*Promusicae, Scarlet/SABAM, SABAM/Netlog, UPC Telekabel, L'Oréal*	Prevent undue restrictions on freedom to receive and impart content by engaging with technological and other contextual factors	Develop law and policy frameworks to ensure that copyright enforcement measures, particularly automated ones, respect copyright exceptions and limitations while taking due account of fundamental rights, societal values and other contextual considerations.

6. Conclusions

The parameters of public debate are increasingly being shaped by private parties, notably online intermediaries. The descriptor, 'new gatekeepers', which is sometimes used to refer to these actors, does not fully capture the complex range of ways in which they control access to information, data and communications in the contemporary online environment. Their operative control of private forums that serve quasi-public informational and communicative purposes means that their actions and omissions can affect an array of fundamental rights, in particular fundamental communication rights, of individuals in different ways. The dominant positions enjoyed by several leading online intermediaries such as Apple, Facebook, Google, Microsoft, Twitter, Yahoo, etc., intensify the impact that their activities can have on individual communication rights – for better or for worse.

In light of the dominant positions and concomitant influence of online intermediaries in the context of public debate – a *sine-qua-non* for democratic society – the question of regulatory oversight of their activities takes on particular importance. A central focus of the present study is the extent to which the European and international fundamental rights framework can shape the scope and substance of privatized law enforcement by online intermediaries. Notwithstanding the existence and endeavours of the Global Network Initiative, the ICT-sector is not governed by an over-arching, comprehensive, effective self-regulatory system. If it were to be developed and accepted across the sector, such a system could – as in other areas of law – complement existing regulatory standards with insightful, participatory, sector-specific operational guidelines and/or codes of practice. In the absence of such a system, however, the focus must turn to more particularized forms of privatized law enforcement at the level of individual entities.

The fundamental rights obligations created by European and international legal frameworks are primarily directed at States. A distinction can be made between negative State obligations (the duty not to interfere with the exercise of fundamental rights) and positive State obligations (the duty to take active measures in order to ensure the effective exercise of fundamental rights). States may not delegate their primary obligation to secure the realization of fundamental rights in practice, either to self-regulatory bodies, or to private parties. Genuine, effective exercise of fundamental rights may require positive measures of protection by States authorities, even in the sphere of relations between individuals, or specifically between online intermediaries and their users. In determining whether or not a positive obligation exists, a fair balance has to be struck between the different rights and interests implicated, as well as the general interest of the community and the interests of the individual or actor involved. These principles have been clearly established by the ECtHR – and also by the CJEU – but formal guidance on how to operationalize and implement them has been limited. In other words, the implications of these principles require further clarification.

This study strives to fill that normative gap, by extrapolating from statements of principle by the two European Courts and, in keeping with the 'living instrument' and 'practical and effective' doctrines of the ECtHR and bearing in mind relevant standard-setting by other bodies, teasing out the implications of these principles for the ICT-sector. The ECtHR has stated that in principle the same criteria apply for determining whether there has been a violation of a State's positive obligations as when there has been a violation of its negative obligations. This means that a State may be found to be in breach of its positive obligations

for its failure to prevent violations of individuals' fundamental rights as a result of privatized law enforcement by online intermediaries. This study has found that criteria that could prove determinative in this respect include the:

- Existence or development by the State of relevant regulatory frameworks;
- Nature of the interference and its intrusiveness (specific techniques of blocking or filtering could prove determinative) and resultant chilling effect;
- Demonstrable degree of involvement or complicity of the State in the interference;
- Adherence to procedural safeguards by the actor (e.g. transparency, adequacy of information; accessibility of terms, conditions and procedures and foreseeability of their consequences, etc.);
- Availability of independent and impartial (judicial) review and redress;
- Dominant position of actor/availability of viable communicative alternatives;

This study has also sought to fill a normative gap by teasing out the implications of positive state obligations in respect of privatized enforcement measures by online intermediaries. In doing so, it has borne the above criteria in mind, as well as the overarching concern to strike a fair balance between competing rights, and focused on the following positive obligations to:

- Guarantee (media) pluralism;
- Create a favourable environment for participation by everyone in public debate;
- Create a favourable environment for freedom of expression for everyone without fear;
- Ensure effective procedural safeguards and effective remedies in respect of the right to freedom of expression;
- Ensure effective procedural safeguards and effective remedies in respect of the rights to privacy and data protection;
- Guarantee that fundamental rights, including intellectual property rights, are fairly balanced against freedom of expression rights.

The suggested implications have both substantive and procedural focuses. They are grounded in the study and they are intended to provide a starting point for a more focused and meticulous discussion on how to operationalize relevant positive obligations of States in the context of self-regulatory or privatized law enforcement measures by online intermediaries.

Bibliography

Literature

Angelopoulos, C., 'Filtering the Internet for Copyright Content in Europe' (2009) *IRIS plus* 4.

Bambauer, D., 'Orwell's Armchair', (2012) 79 *University of Chicago Law Review* 863.

Benedek, W. & Kettemann, M.C., *Freedom of expression and the Internet* (Strasbourg, Council of Europe Publishing, 2013).

Benkler, Y., 'A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate', (2011) 46 *Harvard Civil Rights-Civil Liberties Review* 311.

Boyd, D. & Ellison, N., 'Social Network Sites: Definition, History and Scholarship', (2008) 13 *Journal of Computer-Mediated Communication.*

Brown, I., 'Internet Self-Regulation and Fundamental Rights' (2010), *Index on Censorship,* Vol. 1.

Buergenthal, T., "To Respect and Ensure: State Obligations and Permissible Derogations", in Louis Henkin, Ed., *The International Bill of Rights* (New York, Columbia University Press, 1981), pp. 72-91.

Burrell, R. & Coleman, A., *Copyright Exceptions: The Digital Impact* (Cambridge, Cambridge University Press, 2005).

Cannie, H. & Voorhoof, D., "The Abuse Clause and Freedom of Expression in the European Human Rights Convention: An Added Value for Democracy and Human Rights Protection?", 29 *Netherlands Quarterly of Human Rights* (No. 1, 2011), pp. 54-83.

Chiu, A., "Note. Irrationally bound: Terms of Use licenses and the breakdown of consumer rationality in the market for social network sites" (2011) *21 Southern California Interdisciplinary Law Journal* 167.

Clark, B. & Schubert, M., "Odysseus between Scylla and Charybdis? The ECJ Rules in *L'Oréal v eBay"* (2011) 6-12 *Journal of Intellectual Property Law and Practice* 880.

Dommering, E.J., "De Zaak Scarlet/Sabam: Naar een Horizontale Integratie van het Auteursrecht" (2011) 2 *AMI* 49.

Dreier, T., 'Balancing Proprietary and Public Domain Interests: Inside or Outside of Proprietary Rights?' in Dreyfuss R., *et al*., Eds., *Expanding the Boundaries of Intellectual Property – Innovation Policy for the Knowledge Economy* (Oxford, Oxford University Press, 2001).

Elkin-Koren, N., 'Copyrights in Cyberspace - Rights without Laws', 73 Chi.-Kent. L. Rev. 1155 (1998).

Galperin, E., 'Twitter Steps Down From the Free Speech Party', Electronic Frontier Foundation 21 May 2014. Available at: https://www.eff.org/deeplinks/2014/05/twitter-steps-down-free-speech-party

Guibault, L., *Copyright Limitations and Contracts: An Analysis of the Contractual Overridability of Limitations on Copyright* (The Hague, London, Boston, Kluwer Law International, 2002), Information Law Series No. 9.

Harris, D.J., O'Boyle, M., Bates, E.P. & Buckley, C., *Law of the European Convention on Human Rights* (3rd. ed.) (Oxford, Oxford University Press, 2014).

Horten, M., *A Copyright Masquerade* (Zed Books, 2013).

Howard, P. & Huzzain M., *Democracy's Fourth Wave?: digital media and the Arab Spring* (Oxford, Oxford University Press, 2013).

Hugenholtz, P.B. & Senftleben, M., "Fair Use in Europe – In Search of Flexibilities" (2012) Amsterdam Law School Legal Studies Research Paper No. 2012-39.

Hugenholtz, P.B., 'Codes of Conduct and Copyright Enforcement in Cyberspace', in I.A. Stamatoudi, Ed., *Copyright Enforcement and the Internet* (Alphen aan den Rijn, Kluwer Law International, 2010), pp. 303-320.

Hugenholtz, P.B., 'Copyright, Contract and Code: What Will Remain of the Public Domain?', (2000) 26 *Brooklyn Journal of International Law* 77.

Keane, D., "Attacking hate speech under Article 17 of the European Convention on Human Rights", 25 *Netherlands Quarterly of Human Rights* (No. 4, 2007), pp. 641-663.

Koops, B., Lips, M., Nouwt, S., & Prins, C., 'Should Self-Regulation be the Starting Point?', in B.-J. Koops, M. Lips, C. Prins, & M. Schellekens, Eds., *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners* (The Hague, T.M.C. Asser Press, 2006), pp. 109–149.

Kreimer, S.F., 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link', (2006) 11 *University of Pennsylvania Law Review* 155.

Kulk, S. & Borgesius,F., "Google Spain v. González: Did the Court Forget about Freedom of Expression?", 5 *European Journal of Risk Regulation* (No. 3, 2014), 389-398.

Kulk, S. & Borgesius, F., 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 34 *European Intellectual Property Review* 791.

Leerssen, P.J., 'Cut out by the Middle Man: The Free Speech Implications of Social Media Blocking and Banning in the EU', (2015) *JIPITEC* 6(2), 99-119.

Looms, P.O., "Gatekeeping in Digital Media", Mapping Digital Media Reference Series No. 8, Open Society Media Program, April 2011.

Mac Síthigh, D., 'From freedom of speech to the right to communicate' in Price, M.E., Verhulst, S.G. & Morgan, L., Eds., *Routledge Handbook of Media Law* (London & New York, Routledge, 2013), pp. 175-191.

Margetts, H., 'The Internet and Democracy', in: W. Dutton, Ed., *The Oxford Handbook of Internet Studies* (Oxford, Oxford University Press, 2013).

Margoni, T. & Perry, M., 'Deep pockets, packets, and safe harbours' (2013) (74: 6) *Ohio State Law Journal* 1195.

Marsden, C.T., *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (New York, Cambridge University Press, 2011).

Marsden, C.T., 'Co- and Self-Regulation in European Media and Internet Sectors: The Results of Oxford University's Study', in Moller, C. & Amouroux, A., Eds., *The Media Freedom Internet Cookbook* (Vienna, OSCE, 2004), pp. 76-100.

McGonagle, T., 'User-generated Content and Audiovisual News: The Ups and Downs of an Uncertain Relationship', in S. Nikoltchev, Ed., *Open Journalism, IRIS plus* 2013-2 (Strasbourg, European Audiovisual Observatory), pp. 7-25.

McGonagle, T., 'The Council of Europe's standards on access to the media for minorities: A tale of near misses and staggered successes', in Amos, M., Harrison, J. & Woods, L., Eds., *Freedom of Expression and the Media* (Leiden/Boston, Martinus Nijhoff Publishers, 2012), pp. 111-140.

McGonagle, T., *Minority Rights, Freedom of Expression and of the Media: Dynamics and Dilemmas*, Vol. 44, School of Human Rights Research Series (Antwerp, etc., Intersentia, 2011).

McGonagle, T. & de Beer, K., "*A brave new media world revisited.* Een nog kritischer blik op het nieuwe mediabeleid van de Raad van Europa", 24 *Mediaforum* 2012-11/12, pp. 338-345.

McGonagle, T. & de Beer, K., "*A brave new media world?* Een kritische blik op het nieuwe mediabeleid van de Raad van Europa", 22 *Mediaforum* 2010-5, pp. 146-156.

Montero, E. & Van Enis, Q., "Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: Squaring the circle", *Computer Law & Security Review* 27 (2011) 21-35

Morozov, E., *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs 2012).

Mowbray, A., "The Creativity of the European Court of Human Rights", 5(1) *Human Rights Law Review* (2005), 57-79.

Murphy, T. & Ó Cuinn, G., "Works in Progress: New Technologies and the European Court of Human Rights", 10(4) *Human Rights Law Review* (2010), 601-638.

Nikoltchev S. & McGonagle, T., Eds., *Freedom of Expression and the Media: Standard-setting by the Council of Europe, (I) Committee of Ministers – IRIS Themes* (Strasbourg, European Audiovisual Observatory, 2011).

Nikoltchev S. & McGonagle, T., Eds., *Freedom of Expression and the Media: Standard-setting by the Council of Europe, (II) Parliamentary Assembly – IRIS Themes* (Strasbourg, European Audiovisual Observatory, 2011).

Price, M. & Verhulst, S., *Self-Regulation and the Internet*, (Kluwer Law International, 2004).

Price, M. & Verhulst, S., "In Search of the Self: Charting the course of selfregulation on the Internet and global environment", in Marsden, C., Ed., *Regulating the global information society* (London, Routledge, 2000).

Seltzer, W., 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment', (2010) 24 *Harvard Journal of Law & Technology* 24.

Tambini, D., Leonardi, D., & Marsden, C. T., *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence* (London, Routledge, 2008).

Torremans, L., Ed., *Intellectual Property and Human Rights* (2nd ed.) (Wolters Kluwer 2008).

Trottier, D. & Fuchs, D., 'Theorising Social Media, Politics and the State: An Introduction', in Trottier D. & Fuchs, C., Eds., *Theorising Social Media, Politics and the State* (London, Routledge, 2014).

Urban, J. & Quilter, L., 'Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act', (2006) 22 *Santa Clara Computer and High Technology Law Journal* 621.

Van Hoboken, J., "Legal Space for Innovative Ordering: On the Need to Update Selection Intermediary Liability in the EU" (2009) 13 *International Journal of Communications Law & Policy* 1.

Voorhoof, D., "Het Europese 'First Amendment' – De Straatsburgse jurisprudentie over artikel 10 EVRM: 2004-2009 (deel 2)", *Mediaforum* 2010-6, pp. 186-201.

Wauters, E. *et al*., 'Towards a better protection of social media users: a legal perspective on the terms of use of social networking sites', (2014) *International Journal of Law and Information Technology* 1-41.

Zittrain, J., 'A History of Online Gatekeeping', 19 *Harvard Journal of Law and Technology* (No. 2, Spring 2006), pp. 253-298.

Treaties

Council of Europe

Convention on the Protection of Human Rights and Fundamental Freedoms (ECHR), ETS No. 5, 4 November 1950 (entry into force: 3 September 1953).

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981 (entry into force: 1 October 1985) and its Additional Protocol regarding supervisory authorities and transborder data flows, ETS No. 181, 8 November 2001 (entry into force: 1 July 2004).

European Convention on Transfrontier Television, ETS No. 132, 5 May 1989 (entry into force: 1 May 1993), as amended by its Amending Protocol, ETS No. 171, 1 October 1998 (entry into force: 1 March 2002).

Framework Convention for the Protection of National Minorities, ETS No. 157, 1 February 1995 (entry into force: 1 February 1998).

Convention on Cybercrime, ETS No. 185, 23 November 2001 (entry into force: 1 July 2004).

Additional Protocol to the Convention on cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, 28 January 2003 (entry into force: 1 March 2006).

European Union

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, [2007] OJ C 306/01.

Charter of Fundamental Rights of the European Union, [2010] OJ C 83/389.

United Nations

International Covenant on Civil and Political Rights, United Nations General Assembly Resolution 2200A (XXI), 16 December 1966 (entry into force: 23 March 1976).

Other regulatory instruments

Council of Europe (Committee of Ministers)

CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters.

CM Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers (2011).

CM/Rec(2012)3 on the protection of human rights with regard to search engines.

CM/Rec(2012)4 on the protection of human rights with regard to social networking services.

European Union

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31 (Data Protection Directive).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, [2000] OJ L 178/1 (Directive on Electronic Commerce).

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10 (Copyright Directive).

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights [2004] OJ L 157/45 (Enforcement Directive).

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54.

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (codified version), [2010] OJ L 95/1 (Audiovisual Media Services Directive).

European Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.

European Parliament, Resolution on the freedom of press and media in the world, Doc. No. 2011/2081(INI), 13 June 2013.

United Nations

Human Rights Committee, General Comment No. 16, UN Doc. A/43/40, 28 September 1988.

Human Rights Committee, General Comment No. 31 [80] – 'The Nature of the General Legal Obligations Imposed on States Parties to the Covenant', UN Doc. CCPR/C/21/Rev.1/Add.13, 26 May 2004.

Human Rights Committee, General Comment 34: Article 19 (Freedoms of Opinion and Expression), UN Doc. CCPR/C/GC/34, 12 September 2011.

Case Law

European Court of Human Rights

Ahmet Yildirim v. Turkey, no. 3111/10, ECHR 2012.

Airey v. Ireland, 9 October 1979, Series A no. 32.

Anheuser-Busch Inc. v. Portugal [GC], no. 73049/01, ECHR 2007-I.

Animal Defenders International v. the United Kingdom [GC], no. 48876/08, 22 April 2013.

Appleby and Others v. the United Kingdom, no. 44306/98, ECHR 2003-VI.

Ashby Donald and Others v. France, no. 36769/08, 10 January 2013.

Barthold v. Germany, 25 March 1985, Series A no. 90.

Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland [GC], no. 45036/98, ECHR 2005-VI.

Cengiz and Others v. Turkey, nos. 48226/10 and 14027/11, ECHR 2015.

Chassagnou and Others v. France [GC], nos. 25088/94, 28331/95 and 28443/95, ECHR 1999-III.

Christine Goodwin v. the United Kingdom [GC], no. 28957/95, ECHR 2002-VI.

Costello-Roberts v. the United Kingdom, 25 March 1993, Series A no. 247-C.

Delfi AS v. *Estonia* [GC], no. 64569/09, ECHR 2015.

Demuth v. Switzerland, no. 38743/97, ECHR 2002-IX.

Dink v. Turkey, nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, 14 September 2010.

Editorial Board of Pravoye Delo *and Shtekel v. Ukraine*, no. 33014/05, ECHR 2011.

Fredrik Neij and Peter Sunde Kolmisoppi v. Sweden (dec.), no. 40397/12, ECHR 2013.

Fuentes Bobo v. Spain, no. 39293/98, 29 February 2000.

Haider v. Austria, no. 25060/94, 18 October 1995.

Handyside v. the United Kingdom, 7 December 1976, Series A no. 24.

I. v. Finland, no. 20511/03, 17 July 2008.

Informationsverein Lentia and Others v. Austria, 24 November 1993, Series A no. 276.

Jersild v. Denmark, 23 September 1994, Series A no. 298.

Khurshid Mustafa & Tarzibachi v. Sweden, no. 23883/06, 16 December 2008.

Klaas v. Germany, 22 September 1993, Series A no. 269.

Kruslin v. France, 24 April 1990, Series A no. 176-A.

K.U. v. Finland, no. 2872/02, ECHR 2008.

Loizidou v. Turkey (preliminary objections), 23 March 1995, Series A no. 310.

Malone v. the United Kingdom, 2 August 1984, Series A no. 82.

Manole and Others v. Moldova, no. 13936/02, ECHR 2009.

Matthews v. the United Kingdom [GC], no. 24833/94, ECHR 1999-I.

Michaud v. France, no. 12323/11, ECHR 2012.

M.S.S. v. Belgium and Greece [GC], no. 30696/09, ECHR 2011.

Özgür Gündem *v. Turkey*, no. 23144/93, ECHR 2000-III.

Peck v. the United Kingdom, no. 44647/98, ECHR 2003-I.

Plattform "Ärzte für das Leben" v. Austria, 21 June 1988, Series A no. 139.

Rees v. the United Kingdom, 17 October 1986, Series A no. 106.

Stafford v. the United Kingdom [GC], no. 46295/99, ECHR 2002-IV.

Steel & Morris v. the United Kingdom, no. 68416/01, ECHR 2005-II.

The Sunday Times v. the United Kingdom (no. 1), 26 April 1979, Series A no. 30.

Times Newspapers Ltd. (nos. 1 & 2) v. the United Kingdom, nos. 3002/03 and 23676/03, ECHR 2009.

Tyrer v. the United Kingdom, 25 April 1978, Series A no. 26.

United Christian Broadcasters Ltd. v. the United Kingdom (dec.), no. 44802/98, 7 November 2000.

Van der Mussele v. Belgium, 23 November 1983, Series A no. 70.

VgT Verein gegen Tierfabriken v. Switzerland, no. 24699/94, ECHR 2001-VI.

VgT Verein gegen Tierfabriken v. Switzerland (no. 2) [GC], no. 32772/02, ECHR 2009.

Von Hannover v. Germany (no. 2) [GC], nos. 40660/08 and 60641/08, ECHR 2012.

Weber and Saravia v. Germany (dec.), no. 54934/00, ECHR 2006-XI.

Węgrzynowski and Smolczewski v. Poland, no. 33846/07, 16 July 2013.

Woś v. Poland, no. 22860/02, ECHR 2006-VII.

Young, James & Webster v. United Kingdom, Series A, no. 44, 13 August 1981.

X and Y v. the Netherlands, 26 March 1985, Series A no. 91.

Z. v. Finland, judgment of 25 February 1997, Reports of Judgments and Decisions 1997-I.

Court of Justice of the European Union

Case C-275/06, *Promusicae*, 29 January 2008.

Joined cases C-236/08 to C-238/08, *Google v. LVHM*, 23 March 2010.

Case C-324/09, *L'Oréal v. eBay*, 12 July 2011.

Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011.

Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, 16 February 2012.

Case C-283/11, *Sky Österreich GmbH v. Österreichischer Rundfunk*, 22 January 2013.

Case C-314/12, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*, 27 March 2014.

Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014.

Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014.

Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015.

AG Opinions

Opinion of AG Jääskinen, Case C-324/09, *L'Oréal v. eBay*, 9 December 2010.

Opinion of AG Cruz Villalón, Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* 14 April 2011.

Intergovernmental reports and studies

Council of Europe

Council of Europe, "Report by 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, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282008%2937&Ver=add

Council of Europe Commissioner for Human Rights, "The rule of law on the Internet and in the wider digital world", issue paper, December 2014.

Council of Europe, "Report by 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, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282008%2937&Ver=add.

European Union

Hans-Bredow-Institut, & Institue of European Media Law, Final Report Study on Co-Regulation Measures in the Media Sector, Hamburg/Saarbruken, 2006.

Mandelkern Group on Better Regulation, Final Report, 13 November 2001.

Miscellaneous

Hans-Bredow Institut, *Regulated Self-Regulation as a Form of Modern Government*, Study commissioned by the German Federal Commissioner for Cultural and Media Affairs (Interim Report), October 2001.

McNamee, J., 'The Slide from "Self-Regulation" to Corporate Censorship', Brussels, European Digital Rights (EDRI), 2011.

N-square, *Study on the Scope of Voluntary Law Enforcement Measures Undertaken by Internet Intermediaries* (2012).

Donahue, P., 'Merkel Confronts Facebook's Zuckerberg Over Policing Hate Posts', Bloomberg 26 September 2015. Available at: http://www.bloomberg.com/news/articles/2015-09-26/merkel-confronts-facebook-s-zuckerberg-over-policing-hate-posts

Hansard, HC Deb, 2 April 2014, c957, 2014-04-02. Available online at: http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140402/debtext/140402-0003.htm#140402-0003.htm_spnew12

May, T., Home Secretary's Speech on Counter-Terrorism, *Gov.UK* 24 November 2014. Available online at: https://www.gov.uk/government/speeches/home-secretary-theresa-may-on-counter-terrorism