KLUWER LAW INTERNATIONAL

Copyright Enforcement and the Internet

Edited by

Irini A. Stamatoudi

AUSTIN BOSTON CHICAGO NEW YORK THE NETHERLANDS

Published by:
Kluwer Law International
PO Box 316
2400 AH Alphen aan den Rijn
The Netherlands
Website: www.kluwerlaw.com

Sold and distributed in North, Central and South America by:
Aspen Publishers, Inc.
7201 McKinney Circle
Frederick, MD 21704
United States of America
Email: customer.service@aspenpublishers.com

Sold and distributed in all other countries by:
Turpin Distribution Services Ltd.
Stratton Business Park
Pegasus Drive, Biggleswade
Bedfordshire SG18 8TQ
United Kingdom
Email: kluwerlaw@turpin-distribution.com

Printed on acid-free paper.

ISBN 978-90-411-3346-5

Printed in Great Britain.

Table of Contents

Part III

Codes of Conduct and Copyright Enforcement in Cyberspace

*P. Bernt Hugenholtz**

I. INTRODUCTION

By tradition, copyright enforcement has been a matter for the courts. Copyright holders would take copyright infringers to civil court, where requests for injunctions or claims for damages would be scrutinized by judges applying the rules of due process laid down in the laws of civil procedure. In rare cases of outright 'piracy' (copyright infringement on a commercial scale) prosecutors would bring suspects before criminal courts applying even more strictly circumscribed rules of criminal procedure. No longer. In the digital realm, copyright enforcement is gradually being shifted from the courts and put into the hands of intermediaries applying self-imposed 'codes of conduct'. All over the world, Internet service providers (ISPs) and other online intermediaries are committing themselves, or are compelled to commit themselves, to self-regulatory rules and procedures that seek to provide pragmatic solutions to the massive problem of Internet-based copyright infringement. Such codes might deal with, for instance, notice and take-down procedures that do not exist in background law, or contain obligations to warn infringing subscribers, preserve traffic data, reveal

* Professor, Intellectual Property Law, University of Amsterdam, and Director, Institute for Information Law (IViR).

Irini A. Stamatoudi, *Copyright Enforcement and the Internet*, pp. 303–320.

subscribers' identities or even terminate their accounts. Some codes might go even further, and call for filtering and monitoring of potentially infringing Internet traffic.

National governments and the European Commission tend to applaud, or even foster such self-regulatory solutions, and one can easily understand why. Having the stakeholders sort out the enormous problems of online copyright infringement by themselves saves law makers precious legislative energy and time, especially at the European level, where legislation is increasingly difficult, and deregulation (or 'better regulation') the name of the game. The enthusiasm among governments for self-regulatory codes becomes even easier to understand when one considers the ground rules of the European E-Commerce Directive. The Directive immunizes ISPs from liability for providing access, and rules out any obligation to monitor.[1] This has obviously limited the discretion of national legislatures to come up with legislative solutions. At the same time, content owners worldwide are pressuring online intermediaries into accepting a more active role in the enforcement of copyright online.

While self-regulation undeniably has practical advantages over norm setting by way of legislation, the gradual displacement of civil law remedies by mechanisms of self-imposed enforcement gives reason for concern, particularly since fundamental freedoms of the citizens subscribing to the Internet – notably, rights of due process, freedom of expression and information and right to privacy – are at stake. This chapter critically examines the rise of codes of conduct that deal with copyright enforcement. Its focus will be on codes binding ISPs and other online intermediaries offering similar services, such as providers of user-generated content (UGC) platforms. While solutions in the United States and elsewhere will occasionally be discussed, its regional focus will be on the European Union. Following this Introduction, section II commences by offering a general typology of self-regulation, including discussion of the advantages and disadvantages of self-regulatory approaches and of the legal nature and normative effect of codes of conduct. Section III describes statutory law on copyright law, liability and enforcement, which serves as background law to self-regulatory copyright enforcement schemes. Section IV describes and critically assesses actual codes of conduct dealing with copyright enforcement. Section IV offers conclusions.

II. TYPOLOGY OF SELF-REGULATION

Codes of conduct are the products of self-regulation. In its pure form, self-regulation concerns norm setting and enforcement by private actors, without

1. Directive 2000/31/EC of the European Parliament and of the Council of 8 Jun. 2000 on certain legal aspects of information society services, in particular E-Commerce, in the Internal Market, OJ L 178/1, 17 Jan. 2000 [E-Commerce Directive], Arts 12–15.

the intervention of the state. However, such undiluted self-regulation rarely exists in practice. More often than not the state or legislature is involved in the self-regulatory process, in varying degrees of intensity.[2] Much self-regulation is the product of government pressure put on stakeholders to come up with self-regulation, absent which the government or the legislature will intervene and regulate by statute. Under such pressure private actors will usually prefer to self-regulate.[3] For example, a well-known trade newsletter described the United Kingdom government's attempts in early 2008 to coax ISPs into a code of conduct regarding illegal file sharing as follows:

> On 8 January 2008, at the launching of the government consultation on new copyright exceptions, Lord Triesman, the UK minister for intellectual property, threatened the ISPs with the introduction of new legislation to force them to block illegal filesharing in case they cannot find a voluntary agreement together with the music and film industries by the end of summer. Referring to the Government's attitude towards illegal filesharing, Triesman said 'We're not prepared to see the kinds of damage that will be done to the creative economy,' and regarding the ISPs he added in an interview for The Register 'There is no objective reason why they (rights holders and ISPs) cannot arrive at an agreement. Whether they have the will to do so is another matter.' According to a spokesman for ISPA, the Internet providers' trade association, some 'good meetings' have taken place between the association and film rights owners, but he did not give any specific details on the results.[4]

With *co-regulation* the role of the state is more transparent. Here, the state and stakeholders formally cooperate in the norm setting process. Usually, this cooperation takes the form of the legislature creating a statutory framework 'within which self-governing institutions create rules and administer them'.[5] The resulting rules will often, but not always be subject to government control or oversight. In some cases, governments actually participate in the norm setting process together with private actors in 'a communicative way of decision-making'.[6] For example, the Internet Advisory Board that was established by the Irish government to encourage and supervise self-regulatory

---

2. See M.E. Price & S.G. Verhulst, *Self-Regulation and the Internet* (The Hague: Kluwer Law International, 2005) [Price & Verhulst], 3: 'Self-regulation rarely exists without some relationship between the industry and the state – a relationship that varies greatly.'
3. B.-J. Koops et al., 'Should Self-Regulation Be the Starting Point?', in *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, ed. B.-J. Koops et al. (The Hague: T.M.C. Asser Press, 2006) [Koops et al.], 121.
4. C. Williams, 'Government Piles File-Sharing Pressure on UK ISPs. Minister Threatens Legislation Deadline', *The Register*, 8 Jan. 2008, <www.theregister.co.uk/2008/01/08/triesman_isps_legislation_timetable>.
5. J.P. Mifsud Bonnici, *Self-Regulation in Cyberspace* (The Hague: T.M.C. Asser Press, 2008) [Mifsud], 15.
6. Koops et al., 122.

solutions, apparently played a leading role in facilitating the preparation of a Code of Practices and Ethics that was adopted by the Internet Service Providers Association of Ireland in 2002.[7] Another example is the Dutch Notice-and-Take-Down Code of Conduct, which was published in 2008.[8] The code is a voluntary agreement between Dutch Internet Service Providers and government enforcement agencies, and gives guidance to ISPs on how to deal with allegedly illegal content.

In some cases, self-regulation is the result not so much of governments wielding their power, but of industry pressure. For example, in 2005 the International Federation of Phonographic Industries (IFPI) and the Motion Picture Association (MPA) jointly drafted and published a 'code of conduct' for ISPs, thereby putting pressure on the ISPs to accept some 'social responsibility'.[9] In 2007, a number of major film producers signed an agreement with several large providers of user-generated content services (UGC) in the United States. The agreement sets out so-called Principles for User Generated Content Services,[10] which oblige the UGC service providers to cooperate with content owners on the use of content identification and filtering technologies. The Principles are best understood against the background of ongoing copyright litigation initiated by the content industry against UGC platforms, and thus 'reflect a quid pro quo between copyright owners and content providers: so long as content providers make their best effort to block infringing materials, copyright owners will not sue them'.[11] The arrangement that was concluded in 2009 by the Irish Recorded Music Association (IRMA) and telecommunications provider *eircom*, is an even more direct result of litigation, and can be perhaps better characterized as a settlement than as self-regulation.[12]

A. Advantages and Disadvantages of Self-regulation

Self-regulation has several advantages over regulation by legislation. Norms set by private actors directly concerned are usually geared more precisely to the needs of a specific industry, particularly in specialized fields where government expertise is lacking. Codes set by private actors will often crystallize

7. ISPAI Code of Practice and Ethics, available at <www.ispai.ie/docs/cope.pdf>.
8. Notice-And-Take-Down Code of Conduct, drafted under the auspices of ISOC.nl, available at <http://isoc.nl/info/nieuws/2008-noticeandtakedown.htm>.
9. C. Arthur, 'IFPI Drafts 'Code of Conduct' for ISPs', *The Register*, 12 Apr. 2005, <www.theregister.co.uk/2005/04/12/ifpi_drafts_code_of_conduct>.
10. Principles for User Generated Content Services, available at <www.ugcprinciples.com/>.
11. 'The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance', *Harvard Law Review* 121 (2008): 1387.
12. Briefing note on arrangement between *eircom* and the Irish Recorded Music Association (IRMA) with regard to Copyright Infringement, March 2009 (unpublished but) available at <www.scribd.com/doc/13630351/Eircom-Irma-Briefing-Note-March-2009>.

more quickly than statutory instruments that involve various branches of the legislature. Likewise, self-regulation is more easily revised. This intrinsic flexibility[13] makes self-regulation the regulatory instrument of choice for domains that are in constant flux, such as the Internet.

Norm setting by self-regulation is likely to cost governments relatively little, as compared to the extensive costs of the law making process. This might help to explain why governments tend to promote self-regulation, especially in non-contentious fields. Moreover, self-regulatory codes may provide for more effective and expedient mechanisms of enforcement than statutory law, especially in fields such as intellectual property law that are rarely enforced by the application of criminal law, or suffer from an overworked judiciary. Codes of conduct might provide for rapid and expedient content removal or subscription termination procedures – remedies much quicker than a right holder would have in a civil court, even in summary proceedings. Such quick remedies might also serve as deterrents to would-be infringers, more effective perhaps than the prospect of a protracted civil court case. Also, self-regulatory enforcement may be less costly than enforcement by civil procedure, by avoiding the costs of legal representation.

But self-regulation comes with serious drawbacks as well. The obvious downside of flexibility is legal uncertainty. Self regulation's potential of easy change undermines certainty and often lacks transparency.[14] Additionally, self-imposed codes are usually non-binding, even for the private actors by which they are established, and thereby contribute relatively little to legal certainty. In most instances, recourse to the courts remains a possible avenue for parties not satisfied with the results of a self-regulatory enforcement procedure. In actual fact, the total costs of litigation including an initial round of self-regulatory enforcement procedure might well exceed the costs of normal civil litigation.

As a matter of principle, a more serious draw-back of self-regulation is the lack of accountability of the process of self-regulatory norm setting. Codes of conduct are usually agreed upon between the stakeholders most directly concerned. These stakeholders are likely to protect only their own interests, leaving the more distant interests of, for instance, consumers or the public at large unattended. As Netanel observes:

> Industry self-regulation, a group's regulation of its members' practices with the goal of reducing harmful externalities to outsiders, is notoriously inadequate to its task. As trenchant critics have shown, such self-regulation can only work under conditions of stringent government oversight.[15]

---

13. Price & Verhulst, 9.
14. Koops et al., 124.
15. N. Netanel, 'Cyberspace Self-Governance: A Skeptical View from Democratic Theory', *California Law Review* 88 (2000) [Netanel]: 476.

This 'democratic deficit'[16] becomes particularly worrisome when the norms of self-regulatory instruments directly affect the fundamental rights and freedoms of citizens, such as rights to privacy and freedom of expression. As Price and Verhulst have cautioned:

> [. . .] private censorship can be more coercive and sweeping than public censorship. The dangers of constitutional violation are particularly strong where the self-regulatory entity is acting in response to government or as a means of preempting its intervention.[17]

To avoid that intermediaries become self-appointed censors or tread on the rights of privacy of their end users, self-regulation must be firmly integrated into a legislative framework that guarantees stringent governmental or judiciary oversight. These concerns are reflected in a White Paper on European Governance that the European Commission published in 2001. While advocating self-regulation in the form of co-regulation in certain areas, the Commission warns:

> Co-regulation implies that a framework of overall objectives, basic rights, enforcement and appeal mechanisms, and conditions for monitoring compliance is set in the legislation. It should only be used where it clearly adds value and serves the general interest. It is only suited to cases where fundamental rights or major political choices are not called into question. It should not be used in situations where rules need to apply in a uniform way in every Member state. Equally, the organisations participating must be representative, accountable and capable of following open procedures in formulating and applying agreed rules. This will be a key factor in deciding the added value of a co-regulatory approach in a given case.[18]

B. Legal Nature and Normative Effect of Codes of Conduct

Self-regulation comes in different legal shapes and sizes. Sometimes, a private actor will unilaterally impose upon itself a set of norms that apply only to its own activities. In other cases, private actors will jointly agree on a code or covenant that applies across an entire sector of industry. In many cases, self-regulatory codes are collectively drafted under the auspices of an industry association, as the case is, for instance, with the Code of Practices and

16. Price & Verhulst, 10.
17. Price & Verhulst, 9.
18. European Commission, European Governance. A White Paper, Brussels, 25 Jul. 2001, COM(2001)428, 21.

Ethics that was adopted by the Internet Service Providers Association of Ireland in 2002.[19]

Even if codes of conduct are voluntary arrangements, and are often not binding upon the private parties that have adopted or accepted them, these codes may nonetheless create legal obligations for the parties most directly concerned. Usually, the intermediary's voluntary undertaking will be reflected in the terms of use that contractually bind the users of the service. Through this two-layered structure of private ordering, the norms of voluntary codes may end up as binding contractual provisions. Since online intermediaries often operate in an oligopolistic market, consumers have little choice but to accept the boilerplate terms of use that come with a subscription.[20] Thus the rules that the intermediaries impose upon themselves and pass on to their subscribers become de facto law.

In addition, the substantive provisions of such self-regulatory instruments may have a normative, quasi-statutory effect in a very different way. If intermediaries agree amongst themselves to abide by certain rules, these standards will inevitably play a role in judicial assessments of lawful or unlawful conduct and liability on the part of the intermediaries. For example, the provisions of the Copyright Act of Australia that deal with authorizing infringement (i.e., indirect liability for copyright infringement) expressly require courts to take into account 'whether the person took any reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice'.[21]

More indirectly, the norms of codes of conduct may eventually become statutory law, as legislative solutions will be modelled after self-regulatory approaches, particularly when these are widely supported by the industry. Poignant examples are the 'graduated response' rules that were enacted in recent years in France and the United Kingdom and were largely inspired by industry-wide memoranda of understanding.[22]

C. Self-regulation in Cyberspace

The origins of self-regulation in cyberspace can be traced back to early claims by cyber-libertarians to complete self-governance of the Internet.[23] As Internet guru John Perry Barlow once famously stated in his *Declaration of the*

19. ISPAI Code of Practice and Ethics, available at <www.ispai.ie/docs/cope.pdf>.
20. This raises the question whether consumers can be bound by standard terms that impinge upon basic user freedoms; see L. Guibault, *Copyright Limitations and Contracts. An Analysis of the Contractual Overridability of Limitations on Copyright* (London: Kluwer Law International, 2002).
21. Australian Copyright Act 1968, s. 36 (1A)(c).
22. See text accompanying nn. 45 and 46 below.
23. D.R. Johnson & D. Post, 'Law and Borders – The Rise of Law in Cyberspace', *Stanford Law Review* 48, no. 5 (1996): 1367.

Independence of Cyberspace, 'Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.'[24]

The romantic idea(l) of an Internet without government has however met with considerable scepticism[25] and has now been largely abandoned. Still, the idea that the Internet lends itself to far-reaching forms of self-regulation persists. Since the 1990s, governments in Europe and the United States have advocated self-regulatory or co-regulatory solutions for a spectrum of Internet-related issues, such as privacy, harmful content and domain names management. The reasons for promoting such self-regulation are not so much inspired by ideals of self-governance, as they are by pragmatic considerations: the novelty of the Internet; the absence of a physical (geographical) space where states traditionally exercise their sovereignty; the dynamics of technological change requiring flexible solutions, and the problems of enforcement.[26] Another motivator of self-regulation is legal uncertainty. Wherever states cannot or will not provide the norms that an industry calls for, self-regulation will emerge.

More recently, governments seem to be gradually shifting away from pure self-regulation, preferring instead co-regulatory schemes or normal legislative solutions.[27] Perhaps this reduced reliance on self-regulation is symptomatic of the final stage towards maturity of the Internet. At the European level, the 1990s faith in self-regulation of the Internet is still evident in the E-Commerce Directive that was adopted in 2000. The Directive encourages trade, professional and consumer organizations to draw up codes of conduct at Community level.[28] The European Enforcement Directive of 2004 promotes the development of codes of conduct to facilitate enforcement of intellectual property rights, particularly regarding the labelling of optical discs.[29] At the same time, these and other European instruments illustrate a gradual shift towards state regulation of cyberspace.[30]

---

24. J. Perry Barlow, *A Declaration of the Independence of Cyberspace*, available at <https://projects.eff.org/~barlow/Declaration-Final.html>.
25. Netanel, 395.
26. Mifsud, 9–10.
27. Mifsud, 11.
28. E-Commerce Directive, Art. 16.
29. Directive 2004/48/EC of the European Parliament and of the Council of 29 Apr. 2004 on the enforcement of intellectual property rights, OJ L 157/45, 30 Apr. 2004 [Enforcement Directive], Art. 17. See also Preamble, Recital 19: 'Industry should take an active part in the fight against piracy and counterfeiting. The development of codes of conduct in the circles directly affected is a supplementary means of bolstering the regulatory framework. The Member States, in collaboration with the Commission, should encourage the development of codes of conduct in general.[. . .].'
30. Mifsud, 12–13.

III. BACKGROUND COPYRIGHT LAW

Self-regulation inevitably occurs against a background of statutory law. In the European Union, despite some twenty years of harmonization, this background law is still largely national law. National copyright laws determine what acts on the Internet constitute copyright infringement, and which exemptions possibly apply. National law also governs secondary liability of intermediaries, and copyright enforcement remedies.

The seven directives that have partially harmonized the landscape of copyright and related rights in the European Union have helped to shape the law of copyright in the Member States, particularly in the digital realm. While the Software and Database Directives[31] deal specifically with the protection of computer programs and databases respectively, the Information Society Directive more broadly harmonizes the core economic rights of right holders, in the light of the emerging Internet.[32] Most importantly, in line with the WIPO Copyright Treaty that was adopted in 1996, the Directive requires Member States to introduce an exclusive right of communication to the public that includes a right of making available works online. The Directive leaves no doubt that offering copyright protected content to the public over the Internet, whether by posting works on websites, by file sharing or other means, constitutes copyright infringement, making the person who commits such acts directly liable for infringement.

But the Directive does not touch upon contributory liability, leaving this issue to the Member States. By contrast, the E-Commerce Directive extensively deals with liability of online intermediaries. The Directive immunizes from liability three types of online activity: providing access ('mere conduit'), system caching and hosting.[33] Furthermore, Member States 'shall not impose a general obligation on [Internet] providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity'.[34] The E-Commerce Directive has horizontal application, that is, it encompasses the entire realm of civil and criminal liability, for a spectrum of unlawful acts (torts) ranging from privacy invasion to copyright infringement. Although it immunizes intermediaries under circumscribed conditions, the Directive does not harmonize substantive norms on liability, and providers that fail to qualify for immunity may or may not be held liable, depending on the operation of national law. Contrary to the

31. Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ No. L 122/42, 17 May 1991; Directive 96/9/EC of the European Parliament and of the Council of 11 Mar. 1996 on the legal protection of databases, OJ No. L 77/20, 27 Mar. 1996.
32. Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, OJ No. L 167/10, 22 Jun. 2001 [Information Society Directive].
33. E-Commerce Directive, Arts 12–14.
34. E-Commerce Directive, Art. 15(1).

Digital Millennium Copyright Act of the United States that has served as a model for its safe harbours, the E-Commerce Directive lacks procedural rules on notice and take-down. Whereas some Member States, such as Finland,[35] have autonomously legislated in this area, most countries in Europe, so far, do not provide for statutory rules on notice and take-down, leaving this for the ISPs to self-regulate.[36]

While the E-Commerce Directive immunizes service providers from claims for monetary relief (damages), it does not rule out injunctive relief.[37] For example, Article 14(3) of the Directive, which conditionally immunizes hosting service providers from liability, provides: 'This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.' Whereas the E-Commerce Directive leaves injunctive relief against ISPs to the discretion of the Member States, Article 8(3) of the Information Society Directive of 2001 expressly obliges Member States to ensure 'that rightholders 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'.[38] Similar language can be found in Article 11 of the Enforcement Directive, which harmonizes civil remedies in intellectual property enforcement cases.[39] The Enforcement Directive also obliges Member States to provide for a so-called 'right of information', that is, a court order 'that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who [. . .] was found to be providing on a commercial scale services used in infringing activities'.[40]Arguably, this might be interpreted to include a court order obliging online intermediaries to identify infringing users.

The Directives fail to specify what kinds of injunctive relief are available for right holders against online intermediaries. As implemented in national law, Article 8(3) of the Information Society Directive and Article 11 of the Enforcement Directive have allowed content owners to take legal action

35. Finnish Act on Provision of Information Society Services (458/2002), s. 16, available at <www.finlex.fi/en/laki/kaannokset/2002/en20020458.pdf>.
36. See N. Bortloff & J. Henderson, 'Notice-And-Take-Down Agreements in Practice in Europe-Views from the Internet Service Provider and Telecommunications Industries and the Recording Industry', Workshop on Service Provider Liability organized by the World Intellectual Property Organization (WIPO) (Geneva, 9 and 10 Dec. 1999).
37. E-Commerce Directive, Arts 12(3), 13(2), 14(3).
38. Information Society Directive, Art. 8(3).
39. Enforcement Directive, Art. 11 provides: '[. . .] Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC.'
40. Enforcement Directive, Art. 8(1)(c).

against ISPs, and pressure ISPs into accepting a role in policing the Internet for copyright infringement. As court decisions in the Member States reveal, injunctive relief may come in the form of court orders to terminate Internet accounts,[41] to reveal subscriber data[42] or even to install filtering software.[43] Avoiding such court orders appears to be an important incentive for ISPs to agree to the self-regulatory procedures promoted by the content owners.

The voids that were left by the European and national legal framework – notably, the absence of notice and take-down provisions, and uncertainty as to the appropriate measures of injunctive relief – have fostered a climate that is conducive to self-regulation. As Christina Angelopoulos concludes, '[I]nter-industry voluntary agreements provide ISPs with another kind of ''safe harbour'': when refuge is no longer certain in legislation, ISPs form their own shelter in self-regulation and adjusted ''best practice'' business strategies.'[44] In fact, the E-Commerce Directive expressly invites Member States and the European Commission to encourage the drawing up of codes of conduct 'designed to contribute to the proper implementation of Articles 5 to 15'.

Moreover, as recent legislative initiatives in France and the United Kingdom demonstrate, the legislative gaps at the European level have allowed national lawmakers to create their own 'graduated response' structures of copyright enforcement in cyberspace. Interestingly, the French HADOPI law[45] and the more recently enacted Digital Economy Bill[46] of the United Kingdom both share a history of self-regulation. The French law has its roots in a memorandum of understanding that was agreed in 2007 by major French ISPs, music publishers, film producers, collecting societies and the French government.[47] This memorandum was in turn preceded by a code of conduct that was signed in 2004 by the French music industry, major ISPs and several branches of the French Government.[48]

Similarly, the new British Act is based on a joint memorandum of understanding in an approach to reduce unlawful file sharing that was signed in 2008 by key players in the telecommunications and content industries, the

41. District Court of Amsterdam, 5 Jan. 2007, *AMI* 2007, 55 (*Brein v. KPN*).
42. *Ibid*.
43. District Court of Brussels, 29 Jun. 2007, No. 04/8975/A, published in *Cardozo Arts & Entertainment Law Journal* 25 (2008): 1279 (*SABAM v. Scarlet*).
44. C. Angelopoulos, 'Filtering the Internet for Copyrighted Content in Europe', *IRIS Plus* 4 (2009): 9.
45. LOI n° 2009-669 du 12 juin 2009.
46. Digital Economy Bill, available at <http://services.parliament.uk/bills/2009-10/digitaleconomy.html>.
47. Accord pour le développement et la protection des œuvres et programmes culturels sur les nouveaux réseaux, 23 Nov. 2007, available at <www.culture.gouv.fr/culture/actualites/index-olivennes231107.htm>.
48. Charte d'engagements pour le développement de l'offre légale de musique en ligne, le respect de la propriété intellectuelle et la lutte contre la piraterie numérique, 28 Jul. 2004, available at <www.culture.gouv.fr/culture/actualites/conferen/donnedieu/charte280704.htm>.

regulating authority (OFCOM) and the government. The memorandum of understanding sets out a notification procedure and provides for the possibility of taking technical measures, such as blocking, reducing or slowing down the Internet traffic of infringers.[49]

IV. CODES OF CONDUCT ON COPYRIGHT ENFORCEMENT

A. An Assortment of Codes

While most online intermediaries in Europe and elsewhere have by now subjected themselves to a code of conduct of some sort, not all of these codes deal specifically with copyright enforcement. For example, the Code of Practice of the Internet Services Providers Association (ISPA) of the United Kingdom, quite un-ambitiously, provides: 'Members shall use their reasonable endeavours to ensure the following [. . .] Services (excluding Third Party Content) and Promotional Material do not contain anything, which is in breach of UK law, nor omit anything which UK law requires.'[50]

The Notice-And-Take-Down Code of Conduct that was agreed in 2008 by the Dutch ISPs, deals with 'unlawful content' only in general terms, and rules out its application 'to situations in which other statutory obligations or liabilities apply for intermediaries on the basis of legislation and jurisprudence'. As the explanatory notes explains, the provisions of the Code are without precedent to any liability arising from civil law for acts of copyright infringement by third parties.[51] Some codes even rule out their application to instances of copyright infringement altogether, such as the Code of Practice and Ethics of the Internet Services Providers Association of Ireland, which concentrates instead on spamming and harmful content.[52]

Other codes of conduct do touch upon copyright enforcement, but provide little more guidance for intermediaries than existing background law does. For example, the terms of use that YouTube imposes upon its users, and presumably upon itself,[53] basically repeat the provisions on notice and take-down that exist under the U.S. Copyright Act, as revised by the Digital Millennium Copyright Act (DMCA).[54] The statement of Rights and Responsibilities that govern Facebook's relationship with its users similarly refers

49. Consultation document on legislation to address illicit p2p file-sharing, 37, available at <www.berr.gov.uk/files/file51703.pdf>.
50. ISPA UK Code of Practice, Art. 2.2(1), available at <www.ispa.org.uk/about_us/page_16.html#Legal>.
51. Notice and Takedown Code of Conduct, Explanatory notes to the articles, Art. 1c, available at <http://isoc.nl/info/nieuws/NTD_CodeOfConduct.pdf>.
52. ISPAI Code of Practice and Ethics, available at <www.ispai.ie/docs/cope.pdf>.
53. YouTube, Terms of Service, Art. 8, available at <www.youtube.com/t/terms>.
54. 17 U.S.C 512(c)(3).

to the notice and take-down procedure under U.S. copyright law,[55] as do the Terms of Service of the Google search engine.[56] Note that the safe harbour provisions in U.S. law extend to providers of so-called information location tools, that is, search engines.[57]

By contrast, some codes clearly go further than the applicable background law would require. For instance, several European codes of conduct establish notice and take-down procedures that do not presently exist under statutory law. Likewise, the Code of Conduct of the Canadian Association of Internet Providers (CAIP), establishes a notice and take-down procedure[58] without any material background in statutory Canadian law.

Some codes, more controversially, also establish procedures for the termination of subscriber accounts in cases of repeated copyright infringement. While much of the current debate in this area is focused on France and the United Kingdom – two Member States that have enacted 'three strikes' legislation – it is interesting to note that since its revision by the DMCA in 1998 the Copyright Act of the United States similarly requires termination measures against repeat infringers. Under U.S. law, an intermediary will benefit from the safe harbours provided by the law only on condition that it 'has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; [. . .]'.[59] In line with U.S. law, the YouTube terms provide: 'YouTube will terminate a User's access to its Website if, under appropriate circumstances, they are determined to be a repeat infringer.'

In response to an anticipated revision of the Copyright Act of New Zealand, the Telecommunications Carriers' Forum (TCF) that unites telecommunications carriers and service providers in New Zealand, developed an extensive Copyright Code of Practice designed to assist their members in complying with the proposed new section 92A of the New Zealand Act. This provision would have required ISPs to establish a policy to terminate the Internet accounts of repeat copyright infringers under appropriate circumstances. However, having attracted considerable criticism, the New Zealand Government has announced that section 92A will be amended and not come into force as proposed. Pending this revision, the TCF Copyright Code of Practice remains a draft. Nevertheless, its extensive and detailed rules are

55. Facebook, statement of Rights and Responsibilities, available at <www.facebook.com/terms.php?ref=pf>.
56. Google, Terms of Service, Art. 16, available at <www.google.com/accounts/TOS>.
57. 17 U.S.C 512(d).
58. CAIP Code of Conduct, available at <www.cata.ca/Communities/caip/codeofconduct/CodeConduct.html>.
59. 17 U.S.C. § 512(i)(1)(A) (2000).

illustrative of the proliferation of co-regulatory schemes in this area.[60] Besides setting out in considerable detail procedures of notice and counter-notice, the TCF code also provides rules on what constitutes 'repeat infringement', on 'final warning' and on termination of accounts in cases of repeated copyright infringement. The draft code essentially provides for a rather benign 'three strikes' policy. If a user does not respond to an adequate notice of copyright infringement or does not deny infringement, and this occurs three times within eighteen months, the ISP should terminate the user's account. The arrangement agreed between *eircom* and IRMA in Ireland establishes a more rigorous system of graduated response. Under the Irish arrangement, if an *eircom* broadband subscriber is 'detected of infringing copyright' for a third time, 'the subscriber will be served by *eircom* with a termination notice'.

Possibly the most far-reaching self-regulatory code in the area of copyright enforcement are the Principles for User Generated Content Services that were embraced in 2007 by several UGC services, including MySpace and Dailymotion. The Principles impose on these intermediaries various obligations that well exceed current background law. While neither American copyright law nor prevailing standards of secondary liability require intermediaries to actively filter user-generated content, the Principles obligate UGC Services to '[. . .] fully implement commercially reasonable Identification Technology that is highly effective, [. . .] in achieving the goal of eliminating infringing content'.[61]

B. Assessment

What to make of these codes of conduct? In some cases, where background law is simply restated or rephrased, these codes are innocent reminders of the legal obligations of intermediaries and their users. In other cases, where self-regulatory notice and take-down rules are solidly based in statutory law, they are to be applauded, assuming that these procedures are fairly stated, equitably applied and subject to government or judicial oversight. But, where self-regulatory schemes impose upon the intermediaries, and by implication upon their users, enforcement procedures that have no basis in statutory law, and lack the checks and balances and judicial oversight that come with normal civil procedure, these codes give reasons for serious concern.

Putting copyright enforcement into the hands of private intermediaries presupposes that these private actors are capable of acting as judges of what constitutes copyright infringement, and what not. Of course, in most cases this

60. Telecommunications Carriers' Forum (New Zealand), Internet Service Provider Copyright Code of Practice, Draft 4 Feb. 2009, available at <www.tcf.org.nz/library/2e53bf81-d6c4-4735-9ed0-740e8b2c6af3.cmr>.

61. Article 3, Principles for User Generated Content Services, available at <www.ugcprinciples.com/>.

is not too difficult. But sometimes it is. As various real-life experiments reveal, many ISPs will quickly shut down an allegedly infringing website, even if the claim of the purported right holder is completely bogus.[62] What these experiments reveal is that ISPs are not competent to act as judges, and have no incentive to develop the copyright expertise required to do so. Rather, to keep costs down, they will simply follow the instructions of the alleged right holders. In other words, these codes will lead to risk-avoidance on the part of the ISPs, and thereby compromise basic principles of due process.

What makes such codes even more suspect is that the enforcement measures they authorize (removal of allegedly infringing content, termination of accounts, content filtering, usage monitoring, and disclosure of personal data of suspected infringing subscribers) impinge upon the fundamental rights and freedoms of the users of these services: freedom of expression and information, and right to privacy. While none of these basic (human) rights are guaranteed in absolute terms, restrictions of these rights must be laid down in the law and be proportional.[63]

Several recent court decisions shed light on the question whether such codes are compatible with the European Convention on Human Rights. As to codes of conduct requiring termination of accounts, it is hard to ignore a decision by the French Constitutional Council concerning the HADOPI law. The first version of the law that was originally adopted by the French Assembly, provided for a simple administrative procedure of account termination. This was struck down by the Constitutional Council on the combined grounds that the procedure conflicted with the basic rule of due process, which requires judicial intervention, and that access to the Internet is essentially a human right – part of constitutionally guaranteed freedom of communication.[64]

With regard to filtering obligations, a recent decision of the Court of Appeal of Brussels in the case of *SABAM v. Scarlet* is worth noting. The Brussels Appeals Court questions the legitimacy of imposing upon an

---

62. See the 'Liberty' experiment, <http://pcmlp.socleg.ox.ac.uk/liberty.pdf> and the 'Multatuli project', <www.bof.nl/docs/researchpaperSANE.pdf>.
63. European Convention on Human Rights (ECHR), signed in Rome on 4 Nov. 1950. Art. 10 ECHR 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 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.' Art. 8 ECHR, which guarantees the right to privacy, contains similar language.
64. Constitutional Council, Decision no. 2009-580 of 10 Jun. 2009 <www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf>.

ISP an obligation to filter traffic, in the light of the communication freedoms enshrined in the European Convention on Human Rights and various European directives, and submits searching questions to the European Court of Justice.[65]

With regard to procedures obliging ISPs to reveal to right holders the identities of subscribers suspected of copyright infringement, the decision of the European Court of Justice in the case of *Promusicae v. Telefonica* sets an important standard.[66] While not ruling out that the European acquis allows for national statutory procedures that mandate such disclosure, the ECJ warns that the right to privacy needs to be taken fully into account. In addition, the ECJ calls for proportionality when applying such measures.

What these three decisions clearly indicate is that various enforcement measures currently provided by codes of conduct may run afoul of fundamental rights and freedoms that are guaranteed in national and European human rights law. Concerns over human rights and principles of due process are also amply reflected in the much-debated amendment to the European Framework Directive, one of various directives that harmonize the law of telecommunications in the European Union. Art. 3a of that Directive, as recently revised, reads:

> Measures taken by Member States regarding end-users access' to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law. Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms

65. Court of Appeal of Brussels, 28 Jan. 2010, Case 2007/AR/2424 (*Scarlet Extended v. SABAM*). The Court's main question to the European Court of Justice is: 'Do Directives 2001/29 and 2004/48, read in conjunction with Directives 95/46, 2000/31 and 2002/58 and interpreted with regard to Articles 8 and 10 of the European Convention on Human Rights, allow Member States to authorize a national court [. . .] to order an ISP to put into place, vis-a-vis all of its customers, in abstracto and as a preventive measure, at the expense of the ISP and without limitation in time, a system filtering all electronic communications, both incoming and outcoming, passing through its service, in particular by means of peer to peer software, with the aim to identify the circulation on its network of electronic files containing a musical, cinematographic or audiovisual work to which the claimant alleges to enjoy rights and to then block the transfer thereof, either at the request or at the time it is sent?'

66. European Court of Justice, 29 Jan. 2008, Case C-275/06 (*Promusicae v. Telefónica de España SAU*).

> and with general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to effective and timely judicial review shall be guaranteed.[67]

With broadband access rapidly becoming a public utility in all European households, the codes of conduct binding the intermediaries that provide broadband service have effectively become the law for the citizens of Europe. Therefore, it is submitted that such procedures have no place in self-regulation, unless the relevant provisions are rigorously grounded on a structure of statutory law that adequately warrants basic rights of due process, freedom of expression and information, and right to privacy. Better still, such procedures should be left for the legislatures to regulate, taking into account fundamental rights and freedoms. As the European Commission aptly concludes in its White Paper on European Governance, '[Co-regulation] is only suited to cases where fundamental rights [. . .] are not called into question.'

V. CONCLUSIONS

As this chapter demonstrates, the emergence of codes of conduct that vest in online intermediaries obligations to enforce copyright, either *ex post* (by way of content removal, account termination or personal data disclosure procedures) or *ex ante* (by way of content filtering) raise serious human rights objections. To make matters worse, most of these codes suffer from what critics of self-regulation have termed a 'democratic deficit'. As Price & Verhulst emphasize, '[e]ffective self-regulation requires active consumer and citizen participation at all stages of its development'.[68]

Regrettably, with the codes of conduct on copyright enforcement that are presently emerging, such consumer-citizen involvement rarely, if ever, seems to happen. To infuse these codes with at least a measure of legitimacy, online intermediaries and other stakeholders promoting self-regulatory solutions,

---

67. Directive 2009/140/EC of the European Parliament and of the Council of 25 Nov. 2009 amending Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services, OJ L 337/37, 18 Dec. 2009, Art. 1(b).
68. Price & Verhulst, 10.

might give heed to Article 16(2) of the E-Commerce Directive, which encourages the involvement of consumer organizations in developing codes of conduct that implement the Directive's rules on safe harbour and monitoring.

All this is not to say that codes of conduct have no role to play at all in the realm of digital copyright enforcement. Codes might, for instance, implement certain information duties, as contemplated by the E-Commerce Directive,[69] or standardize terms of use, and thus increase transparency. But when fundamental rights and freedoms are at stake, what we really need, like elsewhere in the law, are duly codified rules and procedures that further the interests of authors and content owners in effectively protecting their rights, while warranting citizens' rights to due process, to free speech and to privacy. At the European level this would imply a revisiting of the rules on ISP liability as enshrined in the E-Commerce Directive. Unlike the Digital Millennium Copyright Act of the United States that inspired its liability rules, the Directive lacks procedural rules on notice and take down. It is high time we started thinking about this now.

69. E-Commerce Directive, Art. 10.