

The Concept of Self Regulation and the Internet

By Monroe E. Price and Stefaan G. Verhulst*

Draft Version

Extract from

Jens Waltermann & Marcel Machill (eds.): Protecting our children on the Internet. Towards a new culture of responsibility. Gütersloh (Germany): Bertelsmann Foundation Publishers 1999

Table of Contents

Introduction

Part 1. Self-Regulation: General Concept and Characteristics

1.1. Defining Self-Regulation

1.2. Regulation and Regulatory Tools

1.3. Benefits and Limitations of Self-Regulation

Part 2. Analytical Framework

2.1. Self and Mediating Institutions

2.2. Government and third party involvement

2.3. Codes of Conduct

2.4. Current Internet Practices and Lessons from other Industries

Part 3. Conclusions and Recommendations

Bibliography

Appendix: Codes of Conduct

Part 3. Conclusions and

* The authors would like to thank Abraham Safdie, David W.J. Canter and Sanjeet Malik for their editorial assistance in the preparation of this article

Recommendations **Erreur! Signet non défini.**

Introduction

This book addresses self-regulation of content on the Internet. Although Internet self-regulation involves many issues, such as e-commerce, technical protocols and domain names management, on-line content controls have initiated most public concern and debate. Throughout this book, emphasis is placed on the operational aspects and design of self-regulation. In this chapter we examine how self-regulatory entities relate to other quasi-legal and state institutions, how it is decided what powers the self-regulatory institutions wield, and how the use of self-regulation can contribute to the more effective and more efficient realisation of both economic and societal goals.

Self-regulation of the Internet has its special qualities, a product of the architecture of the industry, that extraordinary web of computers, servers, telecommunications devices responsible, in large part, for the flexibility, openness and convenience of communication. Self-regulation not only supports the open and decentralised network architecture of the Internet; self-regulation also forms a flexible response to the dynamic and on-going evolution of the sector and the emerging technologies. The development of these Internet technologies has led to outsourcing of operations to private entities and to encouraging third-party or "community" handling of a range of issues including content control.

The issue of content self-regulation on the Internet is a complex one, exacerbated by the inherently transnational nature of the web, the economic and social importance of the newer services, the diversity of cultural norms in this area and the availability of technological tools to affect choices concerning content. The wide range of institutional, technological and social challenges presented by the growth of the Internet has led to government doubts about their capacity to do more than set the broad direction and pace of development. They have increasingly looked to the private sector as a resource for responsibility. The Internet community, seized with the idea of this new means of communication as calling for a very different relationship with government, has taken a similar approach to regulatory design.

In this first chapter, we examine elements of self-regulation that are usually taken for granted. A failure to have a deeper understanding of the mechanisms of self-regulation may hinder the development and implementation of policy. Such an examination also assists in determining the prerequisites and components of self-regulation as part of a comprehensive and systematic process that includes an appropriate role for government and for individual responsibility. In the Internet

context, this exploration also illustrates how self-regulation is a means for ensuring economic growth based on emerging network technologies and an optimal combination of speech rights consistent with suitable protection of community interests.

Part 1. Self-Regulation: General Concept and Characteristics

1.1. Defining Self-Regulation

The initial problem of every approach to self-regulation lies with definition. There is no single definition of self-regulation that is entirely satisfactory, nor should there be. Self-regulation evolves as the nature of the Internet alters. Different profiles of self-regulation emerge that adjust to the varying aspects of the Internet that are regulated. Self-regulation has and will continue to have different meanings from sector to sector and from state to state, internationally. Furthermore, whatever its implication or suggestion, self-regulation is almost always a misnomer. It hardly ever exists without some relationship to the state; a relationship that itself varies greatly. The meaning of self-regulation shifts depending upon the extent of government coercion or involvement and upon accurate public perceptions of the relationship of private sector and state.

For these and similar reasons, there is a great hazard: governments, industries and users employ the term "self-regulation" frequently, almost indiscriminately. It is assumed to have a pre-determined meaning when it does not. A study on self-regulation in the Media Sector and European Community Law noted that "The term "self-regulation" is often used as a matter of course, as if it were (1) a specific and defined term, and (2) an equally specific and defined regulatory practice. Yet in general, this is not the case" (Ukrow 1999: 11). From the outset, then, there needs to be an exploration of the variety of meanings of "self-regulation" and the implications of each grouping of them for the better management of social concerns with the new technology.

Different variables

Larry Irving, US Assistant Secretary of Commerce, observed: "At one end of the spectrum, the term is used quite narrowly, to refer only to those instances where the government has formally delegated the power to regulate, as in the delegation of securities industry oversight to the stock exchanges. At the other end of the spectrum, the term is used when the private sector perceives the

need to regulate itself for whatever reason -- to respond to consumer demand, to carry out its ethical beliefs, to enhance industry reputations, or to level the market playing field -- and does so"¹. Even here, the range of variable meanings emerges. Because "self-regulation" is thought to exist when private entities have been commanded to act or become the delegates of state power, the intertwining of state and private industry is implicitly recognised, although the "governmental nature of self-regulation" may differ across sectors (Baldwin/Cave 1999: 125). Questions arise: these include the propriety and clarity of delegation, the circumstances under which state functions can or ought to be carried out by private groups, the division of power and responsibility between the state and private groups. On the other hand, as Secretary Irving suggests, the private sector "perceives the need to regulate itself." The source of that need is often the threat of public regulation or a societal demand for increased responsibility by the private sector or economic factors. Other variables may include the extent of the role played by self regulators, the degree of binding legal force that attaches to self regulatory rules and their coverage of an industrial sector (Baldwin/Cave 1999: 126). These areas of indeterminacy are grounds for a statement in a recent Bibliography on Self-Regulation on the Internet prepared for the OECD: "while there is broad consensus that self-regulation of the Internet is critical to its future growth, there is little consensus about how to achieve or implement a self-regulatory regime" (Internet Law and Policy Forum 1998).

Essentialist Approach

To appreciate these various meanings and dimensions of self-regulation, the concept must be further dissected. An essentialist approach to self-regulation would require that all elements of regulation-- formation of norms, adjudication, enforcement and others--be self-generated. Not only the rules that govern behaviour, but the mechanisms for their administration would arise from those whose behaviour is to be governed. Even "subcontracting" of rules might violate the purest ideal of self-regulation if the contractor is the government. Rules must be auto-generated in that ideal model. But it is rare that any form of self-regulation, save for cartelization, really exists wholly independent of the force of the state and this may be especially true where the field of regulation involves content control on a medium of expression. Huyse and Parmentier distinguish between subcontracting (where the state limits itself to setting the formal conditions for rule-making while leaving it entirely up to the parties to shape the content), concerted action (where the state not only

¹ When introducing a collection of papers analysing the prospects of self-regulation for protecting privacy (National Telecommunications Information Administration 1997).

sets the formal, but also the substantive conditions for rule-making by one or more parties) and incorporation (where existing, but non-official norms become part of the legislative order by insertion into statutes or by declaring the product of private negotiations generally binding for a whole sector) (Huyse/Parmentier 1990: 260). Nor is the involvement of third parties in a self-regulatory body precluded. The important quality is the vector: maximising private or self-regulation as a supplement, substitute, or delegate of the state.

Self-Regulation and Other Regulatory Models

Another, though closely linked, way of defining self-regulation is determining its particular place and role among other regulatory models². In reality the behaviour of industry players can in essence be governed and controlled through three forms of economic and social organisation: government organisation, industry self-organisation; and market organisation. Where any particular form of regulation falls on this spectrum depends largely on who gives impetus to its development. Moreover regulation encompasses varying degrees of legal force and formal organisation. From what we have already said, it will be apparent that there is no clear demarcation between self-regulation and government regulation. The principal types constitute a continuum along which regulation is more or less formalised, with government or public regulation being the most formal (the so-called command and control type of regulation) and where non-compliance may lead to public or private law sanctions; and market organisation (*laissez faire* approach) being the least formal and 'compliance' based upon voluntary action. In practice, however, the three forms overlap and create mutual inter-dependencies as a result of market or policy failures, or even wider public concerns - such as the protection of minors - which cannot be addressed purely by one form or another. Sinclair argued that "much of the current debate has been characterised by a choice between two mutually exclusive policy options: 'strict' command and control on one hand, and 'pure' self-regulation on the other. In fact, there is a much richer range of policy options, with most falling somewhere between theoretically polar extremes" (Sinclair 1997: 529). Many authors have concluded that self-regulation and formal legal systems work best when they are combined (Doyle 1997: 35-42). Furthermore, the mix between the two should shift depending on changes in the environment. Such changing conditions might include technological innovations. As an example, the evolving nature of the Internet has not only led to calls to regulate the Internet in a certain way

² Joseph Rees, somewhat idiosyncratically likens the general regulatory system in his landmark book *Reforming the Workplace*, to the proverbial iceberg: the tip being government regulation, while the massive body represents

but has also challenged the current regulatory regimes in place for other communications systems such as broadcasting and telecommunications. In this way, styles of regulation on the Internet might decrease government regulation and accelerate the shift for greater self-regulation in other media areas. Two-tiered regulation is especially relevant in industries and areas that are complex and transnational in character, with content regulation being an example. It is convenient and logical to consider these co-regulatory mechanisms as a form of self-regulation. Hoffmann-Riem calls this "regulated self-regulation" (Hoffman-Riem 1996).

Self-regulation versus de-regulation and non-regulation

Self-regulation is different from de-regulation or non-regulation. De-regulation directly aims to remove any regulation perceived to be excessive and to hinder market forces. Self-regulation does not aim primarily to dismantle or dispense with a framework for private activity, but rather to change the actor who establishes this framework (Ukrow 1999: 15). Self-regulation is no alternative or substitute for elements of direct regulation, such as antitrust (Breyer 1982: 157). It is a technique, not a prescription for overall regulatory institutional design (Prosser 1998: 271). Considering self-regulation as the antithesis of legal regulation is thus far too simple a characterisation of the limits to law. We are concerned here, rather, with whether self-regulatory bodies can be an alternate significant source of "law" in the Internet. What we see, every day, is greater social demand for some form of control or supervision of what seems, inherently, to be beyond governance. This significant gulf between community aspiration and perceived limits on government capacity forces a thorough and almost painful search for each possibility of finding a remedy. Innovation of regulatory design is required in the Internet, to resolve this dilemma.

Comparative approaches

Few existing discussions of self-regulation on the Internet pay attention to disparate meanings of self-regulation in various states. The very history of the relationship between business and government is so different in the major Internet states (we may look at the US, Germany and the UK as a sample). It is inevitable that the patterns of "self-regulation" will differ accordingly. An international practice of self-regulation may emerge but it will have to be, in the first instance, an accumulation of national and regional experiences. Each state has different social demands, each

society's great array of private regulatory systems (Rees 1988: 6).

state has a different constitutional structure, and each state has different traditions of industry-government co-operation in the fields of media and speech. No account of the emergence of self-regulation can be complete that fails to be not sensitive to these critical distinctions in practice. The expectation, function, structure and culture of self-regulation in the media is very different in Europe from the United States and in Germany from the United Kingdom, to give just two examples. One study of self-regulation and self-generation of standards (Canada and United States) demonstrated marked differences in the scope of co-operation with the government, shared standards, and the notion of self-regulation as a social and collaborative act (McDowell/Maitland 1998). In the United States, partly because of the First Amendment tradition, self-regulation is distinctively a form of avoidance, confrontation, and studied separation from government. A comparative overview of self-regulation systems in all EU Member States within the media identified clear differences in meaning and structure of the self-regulatory systems within the individual EU Member States and in a comparative overview of these systems (Brohmer/Ukrow 1999). An understanding of these different traditions will assist a) in building common approaches where appropriate and b) in avoiding misunderstandings about the capacity of self-regulation across systems.

1.2. Regulation and Regulatory Tools

It is frequently said that the Internet is unregulable, or that regulation is beyond the control of the nation-state. The assumption of this book, and, of course, of this chapter, is that not only is some level of regulation possible, but that it can be undertaken by those involved in operating the Internet (Goldsmith 1998). It is important, however, to be clear about the differences between regulation by government and self-regulation by those largely operating apart from government. Regulation by government always implies the use of government power to ensure certain actions by third parties. Self-regulation, on the other hand, consists of a series of representations, negotiations, contractual arrangements and collaborative efforts with government. Self-regulation on the Internet is a subtle and changing combination of all of these forms of activity. Further, self-regulation can be seen as that range of activity by private actors undertaken to prevent more intrusive, and more costly action by government itself. In that sense, self-regulation can be explained as a collective economic decision, an intersection of maximisation of profit and expressions of public interest.

Justifications for and Objectives of Regulation

The starting point of every regulatory intervention, including self-regulation must be the policy objective, not the means of achievement. In other words, the need and rationale for the rules and techniques to be imposed must first be identified. Justification for intervention arises out of an alleged inability of the marketplace to deal with particular structural problems. Other rationales are often brought up in political debate, (and the details of a program often reflect only political force). Market failure forms the main rationale behind self-regulation, but a distinction must be made between economic self-regulation and social self-regulation. While the former is concerned with the adjustment of markets or other facets of economic life, the latter "aims to protect people or the environment from the damaging consequences of industrialisation" (Hawkins/Hutter 1993: 199). Social self-regulation is thus usually taken to include mechanisms whereby firms or their associations, in their undertaking of business activities, seek to assure that unacceptable consequences to the environment, the workforce, or consumers and clients are avoided. Media regulation and especially content self-regulation, falls clearly under this category. Many scholars have listed the reasons why the media should be regulated³. European Commissioner Oreja summarised these reasons as follows:

"In order to give an answer to this question, the starting point is, of course, to recognise the crucial role that media play in our society. The role of the media goes much further than simply providing information about events and issues; media also play a formative role in society. That is, they are largely responsible for forming the concepts, belief systems and even the languages visual and symbolic as well as verbal - which citizens use to make sense of, and to interpret the world in which they live... There are a certain number of public interest objectives which should be preserved in our societies, and which have a European dimension. In my opinion, these could be summarised as follows: ensuring plurality of ownership; ensuring fair and effective competition; ensuring diversity of content; protecting individual rights to privacy, free speech, etc; protecting intellectual property rights; maximising individual consumer choice and access to information, and, very importantly; ensuring a high level of protection of minors and human dignity" (Oreja 1999).

³ Hoffman-Riem lists among the fields of supervisory action *inter alia*: pluralism, diversity, fairness, and impartiality; social responsibility; maintenance of high quality programming and of cultural and linguistic identity; coverage of important events; protection against abuse of market power; strengthening national and regional industries; protection of consumers; and maintenance of standards in matters of violence, sex, taste and decency (Hoffman-Riem 1996).

Much discussion about the development of the newer communications services and the growing globalisation suggests that new technology challenges these rationales. The European Green Paper on Convergence differed: "The fundamental objectives underpinning regulation in the Member States are not undermined by convergence" (European Commission 1997). "Nevertheless," it continues, "the nature and characteristics of convergence as well as the perceived need of industry actors for regulatory intervention to be limited and closely targeted, should lead public authorities at both a national and a European level to re-examine the role and weight of regulation in a converging marketplace". These differences led to the call for self-regulatory approaches. Public interest objectives do not become irrelevant or invalid as a result of technological change. The regulatory challenge within an Internet setting is thus to find appropriate legislative and other mechanisms to safeguard these policy objectives. A functional approach is needed, one which does not depend solely on technology or forms of delivery, but which recognises the nature of the service and the character of the audience receiving it. However, in identifying the most appropriate legislative approach for controlling Internet content two areas of complexity have to be taken into consideration. The first refers to defining the types of content that is unacceptable and/or illegal. The second is related to the different methods or platforms of exchanging information on the Internet.

Harmful and illegal content

A discussion of illegal, harmful or offensive content is always a complex matter (OECD 1997a) not unique to the Internet, even, or especially, in terms of definition. Several EU documents have outlined that it is necessary to differentiate between these categories of content (European Commission 1996) but a fully satisfactory definition is not given. The "Green paper on the protection of minors and human dignity in audio-visual and information services" (European Commission 1997b) produced broad agreement on objectives and the action to be taken within Europe. Generally, the concept of "illegal" seems a relatively simple reference to content that is contrary to law. However this becomes a particularly difficult issue in the international context, where what is illegal in some countries is not necessarily illegal in others. It was only recently that Japan's lower house of Parliament banned the production and sale of child pornography. Furthermore this question can be exacerbated in a discussion of civil and criminal law, where "illegal" only refers to that which is a criminal offence and "harmful" might indicate that content which raise civil law issues because of "harm" to another party. What is considered to be harmful or

appropriate depends on cultural differences and can be distinct according to different age groups. All this has to be taken into account in defining appropriate approaches to protect children against undesired material whilst ensuring freedom of expression.

Internet Platforms

It is also important to keep in mind that (world wide) web pages are only one of the platforms by which content is exchanged on the Internet. Other methods of information exchange include e-mail, ftp, newsgroups and real-time chats. As the KPMG review of the Internet Watch Foundation highlighted, each route has different characteristics and is used for different purposes and may require different regulatory and protective approaches. Chat and newsgroup platforms were, for instance, thought to be the most widely used communications platform on the Internet by paedophiles because of the difficulty in "traceability". Moreover filtering and blocking of such dynamic content has proven to be problematic and in some case impossible. All this confirms that a multiple approach of regulatory tools will be necessary to control Internet content satisfactorily.

Self -Regulatory Tools

A wide array of self-regulatory tools have proven track records as substitutes for government regulation. They assume many forms, ranging from social control to formal contracts. Codes of conduct, voluntary standards, contractual provisions, accreditation, third-party certification, audits, best practices and performance goals and objectives have all withstood scrutiny in lieu of prescriptive regulation in a variety of industry settings, including the media. Dispute resolution is also an important element within a self regulatory regime for the Internet (Katsh 1996).

Codes of practice or good conduct embodying mutual obligations by competing actors have an important role to play, but one of the most distinct means of enhancing protection and free speech on the Internet is the use of filtering and blocking mechanism as described in the essay in this book by Balkin and Noveck. This is not to say that legal controls are unimportant but the shift from "hard law to software" (Wacks 1997) can clearly be considered as an empowerment of user's choice, (as opposed to an analogue broadcasting setting). Hence the major response to the call for self-regulation involves processes that promote filtering and rating systems. The institution of hotlines and complaint handling procedures by industry actors is also an important element of content self-regulation on the Internet. Hotlines - as Burkert describes in this book- can provide a mechanism for users to report illegal or harmful content that they see on the Internet. Based upon a

public-private partnership they can have a crucial evaluation and monitoring function. In what follows later in this discussion, codes of conduct will be addressed in greater detail. There are a number of industry initiatives underway directed at developing codes of conduct and a number of national governments specifically endorse codes as a front-line mechanism for addressing content issues. Moreover codes of conduct, as discussed above, may also offer a solution to content platforms that are difficult or impossible to filter and/or block, such as newsgroups or e-mail.

Regulatory Process

Finally, in examining the design of self-regulation, one should also examine different components of the regulatory process which include: (i) policy making, i.e. enunciating principles that should govern enterprises, (ii) legislation, i.e., defining appropriate rules; (iii) enforcement, i.e., initiating actions against violators; and (iv) adjudication, i.e., deciding whether violation has taken place and imposing an appropriate sanction. The point here is to determine, in each particular version of the exercise of regulation, how the roles are divided between the state and industry (Campbell 1999). For example, an industry may be responsible for the definition of standards for content (through developing a code of practice) but leave enforcement to the government. Industry may put its mark on official state legislation through effective lobbying, using state power to obtain results that could not be gained through private agreement. Self-regulation often means a division in which certain kinds of behaviour (incitements to violence, for example) are defined as prohibited by the state, while other kinds of speech behaviour (indecent conduct) are defined, labelled and policed by the industry. Similarly, enforcement may be divided with the state prosecuting for certain speech and the self-regulating entity self-policing and removing other kinds of speech.

1.3. Cost-benefit analysis

A fashionable way of looking at the characteristics and merits of self-regulation is to examine how it complements and addresses the limitations of government regulation. The increasing significance of self-regulatory mechanisms suggests that they offer a number of benefits that cannot be achieved through government regulation. Within the debate on self-regulation, however, a key question arises as to whether and in what ways self-regulatory systems can effectively monitor and control the behaviour of market players without generating the bureaucratic and legal costs of traditional regulatory regimes.

Costs

Implementing and complying with regulation entails significant costs, and efficiency losses associated with regulation can be high. Moreover, government regulation can be a blunt instrument and impose unintended costs (on the customers of other, competitive industries) without any tangible benefits (Ministry of Consumer Affairs, NZ, 1997). In contrast with command and control type of regulation, the "voluntary" nature of self-regulation implies, sometimes misleadingly, that the costs associated with compliance are lower and fall on those markets at which regulation is targeted.

It is however naive to suggest that self-regulation does not itself involve significant costs. For any system, regulatory or self-regulatory, costs are determined by a combination of the policy goals they envisage and the structures and dynamics of the economic and social activities they regulate. Monitoring and evaluative costs otherwise assumed by governments may be incurred directly by individual companies or indirectly by industry associations who will also generate significant amount of third-party costs associated with governmental compliance procedures. To some limited extent, new technology automates regulatory controls, procedures and compliance requirements, decreasing regulatory costs. But that would be true for direct regulation as well as self-regulation.

Enforcement and "Free Riders"

The very nature of a voluntary system, however, potentially creates a "free-rider problem" (OECD 1998) where some actors expend significant resources on the development, monitoring and implementation of codes and standards while others ignore their existence. This situation may not be entirely disadvantageous to more resourceful actors, as they can set benchmarks that can convey benefits in terms of consumer confidence and recognition in market formation and social responsibility. Commercial and social prominence is critical for the success of the major actors on the Internet as it is in any other medium (AOL is an example of the process⁴). And once a critical mass of participants has been reached, a "voluntary" system of codes and controls can become very hard to evade because of increased peer-pressure and public expectations.

Self-regulation can quickly become moribund without strong and committed support for its development, implementation and enforcement. To be a living and working instrument, a Code of

⁴ AOL's recent advertising campaign assures customers of their ability to determine access to content, using AOL's age referenced system (<http://www.aol.com>). AOL has also enacted a "Safe-Surfing" campaign, outlining basic

Practice or equivalent must, in practice, be implemented with the agreement of the industry sector to which it applies. Whether governments may need to have reserve powers to ensure the effectiveness of self-regulation depends - as will be seen below- largely on this collaboration among industry players and on the type of societal goals and the need to ensure that users are aware of their protection. But in any case "voluntary" and "preventive" self-regulation can be a sensible strategy to prevent considerable time and financial resources from being bound up in compliance activities.

Expertise and Information

Another major limitation of traditional government regulation is that government agencies may lack the information and technical competence necessary to make the best policy decisions. On the Internet a vast amount of data is collected by network operators, Internet Access (IAP) and Service Providers (ISP) on the use and abuse of networks. This information can consist of basic personal and commercial data such as users' names, addresses and also confidential information collected by technologies integrated into the network. Tracking of service site visits activity by users on a Web site is probably the most common data collected by IAPs and ISPs. The collection of these types of data has initiated competitive and consumer privacy concerns that need to be addressed (Birks 1997). The ability to gather this information in itself has opened a wide debate about the liability of these "mediating institutions"⁵. Still, the capacity enables the industry to identify and monitor key areas of content concern in a more effective way than government agencies would be able to do. The expertise that can only be effectively contributed and processed by the industry-actors themselves can thus be mobilised within a self-regulatory structure to devise, subject to careful safeguards "responsive regulation" (e.g. codes of conduct). Self-regulation should not, however, be a pretext for a new onslaught on privacy.

Free Speech and Globalisation

Self-regulation has the seeming benefit of avoiding state intervention in areas that are sensitive in terms of basic rights such as freedom of speech and information while offering social

parental options in relation to children and Internet use (<http://www.safesurfin.com/>).

⁵ The case against Felix Somm, managing director of CompuServe Germany, in Bavaria highlights these dilemmas facing governments, law enforcement agencies and the judiciary when defining liability for on-line content with regard to Internet service providers. On 28 May 1998, the Munich Judge imposed a two year suspended sentence on Felix Somm. This was the first time in Germany that an online company manager had been held responsible for images available through the firm's gateway to the Internet. (<http://www.cyber-rights.org/isps/somm-dec.htm>). Goldsmith discusses the problems of legislative attempts at regulating content. (Goldsmith 1998: 1224-1226; Delacourt 1997).

responsibility, accountability and user protection from offensive material. But private censorship can be more coercive and sweeping than its public form. And the dangers of constitutional violation are particularly striking where the self-regulatory entity is acting in response to government or as a means of preempting its intervention.

Self-regulation may better absorb the transnational conflicts inherent in the global architecture of the Internet. An emphasis on self-regulation may be a more effective alternative wherever one state is highly dependent on consensus with other states. Furthermore government regulation can be inflexible and not as adaptable to the rapid changes taking place in the Internet as other policy alternatives. Robert Pitofsky, Chairman of the Federal Trade Commission (US), explained recently that "[I]legitimate and fair self-regulation will become more important as the economy grows faster than government regulation" (Pitofsky 1998). He also referred to the fact that self-regulation sometimes is more "prompt, flexible, and effective than government regulation" and that "the judgement and experience of an industry also is of great benefit, especially in cases where the government has difficulty defining 'bright-line rules'. On-line content is clearly such a case.⁶

Thus, the professed advantages of self-regulation over governmental regulation include efficiency, increased flexibility, increased incentives for compliance, reduced cost, and minimised government intrusion in the speech field. However, a number of risks and limitations, besides the ones already listed, are also associated with self-regulatory approaches especially if they need to fulfil public interest goals as in the case of policing Internet content.

Democratic Deficit and Accountability

The "democratic deficit" or "corporatist character" (Schmitter 1985) of self-regulation in comparison with state regulatory activities can be seen as an important cost. The shift -within self-regulatory arrangements- of traditional public task fulfillment from specific and democratically legitimate regulatory institutions into a sector that consists primarily of private associations occurs at the expense of democracy and accountability. The acquisition of power by groups that are not accountable to the body politic through the conventional constitutional channels may constitute an abuse. As John Braithwaite has put it: "Self-regulation is frequently an attempt to deceive the public into believing in the responsibility of an irresponsible industry. Sometimes it is a strategy to give the government an excuse for not doing its job" (Braithwaite 1993: 91).

⁶ The U.S. courts recently invalidated the Communications Decency Act and granted a preliminary injunction against enforcement of the Child Online Protection Act. (*Reno v. ACLU*, 117 S.Ct. 2329 (1997); *Reno v. ACLU*, 31

It is clear that legitimacy plays an important role within the debate about government versus self-regulation. Part of the discussion is linked to the responsibility of mediating institutions to ensure transparency, accountability and consultation with interested parties. These are in general not perceived by the private sector as their primary objectives. Therefore, ensuring accountability when public interests are concerned should be a major concern in the design of a self-regulatory regime. Effective self-regulation requires active consumer and citizen participation at all stages of development and implementation. Without user involvement, a self-regulatory mechanism will not accurately reflect user needs and will not be effective in delivering the standards it promotes. It will fail to create confidence.

Self-regulatory institutions may not impose meaningful sanctions on industry players. Self-regulatory standards are, according to critics, usually weak, enforcement is ineffective and punishment is often secret and mild. If there is insufficient commitment to an enforceable code, the power of state regulation to effectively sanction contravention may be preferable. Finally, self-regulation can have an adverse impact on competition and market efficiency if the sector concerned attempts to use self-regulation as a way of restricting competition by, for example, limiting entry, driving up prices, or setting minimum standards of trading conduct that have little relevance to the needs of consumers. As a response to these concerns within the media field, European Commissioner Oreja recently stated that "self-regulation should not be used by major dominant operators to define 'rules of the game' that are best suited to their own interest to the detriment of small or more recent competitors"⁷ (Oreja 1999; Page 1987).

Part 2. Analytical Framework

It is difficult to deal with each and every area of indeterminacy involved in defining and then implementing notions of self-regulation. Also, it is impossible to consider each benefit and weakness self-regulation and its specific mechanism may have under each circumstance. Three areas, however, can be deployed to demonstrate the variety of meanings and implementations that can exist.

F.Supp.2d 472 (1999)).

⁷ However the opposite has also been claimed. One of the main reasons why self regulation was introduced in the financial services in Britain was not only that it would lead to higher standards of business conduct, but that it was thought less likely than government regulation to inhibit innovation and international competitiveness (Rees/Cunningham 1997).

The first involves the scope of self-regulation: what, in a shorthand way, constitutes "the self." Self-regulation by business often means how businesses police themselves, what standards they use for their own conduct and what steps they deploy to see that those standards are followed. A second area focuses on what is meant by the "regulation" side of "self-regulation." While the inquiry into "self" deals with the issue of whose conduct, whose speech, whose uses are affected, and by whom, "regulation" deals with the tools that are used (such as denying access to those whose use is considered harmful) and the rationales or justifications behind the selected regulatory design. Mandating ratings or providing incentives for rating could be considered, in this sense, a form of regulation.

Finally, one needs to examine the background requirements for self-regulation, the varied institutional relationships that exist between industry and government, all within the self-regulatory banner. These relationships become even more complex in an Internet setting because of the need for international consultation and co-operation among states and private actors. States, industry and user associations are recognising that the impact of any regulatory action will, in many instances, extend far beyond their frontiers. This is particularly relevant in the case of content on the Internet, given the significant role of culture and social values in these issues.

2.1. Self and Mediating Institutions

The Self of Self-Regulation

The Internet is a consummate demonstration of the complexity of determining what ought to be included in the "self" of self-regulation. The Internet prides itself on being an autonomous interconnected, totally decentralised, set of communications networks. It includes a cornucopia of institutions that partake of self-regulatory characteristics. Standards and protocols are established by such entities. The process of establishing, registering and managing domain names is such a self-regulatory mechanism. Voluntary institutions, generated by the Internet and not by government, are the very backbone of efforts to deal with harmful content. W3, the entity seeking to develop protocols for websites that -among other things- can serve as the foundation for rating and filtering systems, is a paradigm of self-regulation. Self-regulation can refer to unmonitored, unaudited efforts by the single firm and it can extend to an elaborate process in which all users participate as well as all firms, with government playing roles that range from design, coercion, auditing, monitoring or acquiescence.

Individual Versus Collective Self-Regulation

Within this wide range of dimensions of the "self", it is important to distinguish between individual firm self-regulation (where an entity regulates itself, independent of others) and self-regulation by groups. Self-regulation may speak to the specific actions of each actor, but it often refers to a collective constraint by which individual actors are bound. In the Internet setting, one could consider as a matter of individual self-regulation the decisions by each entity that operates as a service provider or a bulletin board or program supplier as to what they will post or what rules they will consider themselves governed by, including rules to rate or label content. Several major service and content providers (such as AOL, MSN, and others⁸) have developed explicit guidelines and user protection guarantees (especially for minors), often labelled "Netiquette" in order to establish and maintain confidence among their users.

This approach is by no means feasible only for large multinational enterprises though only such firms may have sufficient resources to reflect by a range of nationally defined tastes and requirements. In practice, in terms of social response to the Internet, self-regulation implies some degree of collective or community constraint, rules imposed upon each member or actor by an entity created by some or all the actors often under pressure from government. This collective action or, in some cases, the creation of a private regulatory entity, engenders outcomes that would not be reached by individual behaviour alone. As such self-regulation is a process of "collective self-governance". It describes the situation of a group of persons, institutions or bodies, acting together, performing a regulatory function in respect of themselves and others who accept their authority.

Industry Self-Regulation

Industry self-regulation may also be described as a regulatory process whereby an industry-level (as opposed to a governmental or firm-level) organisation sets rules and standards (codes of practices) relating to the conduct of firms in the industry. This definition implies that industry self-regulation requires firms in the industry to decide to co-operate with each other, through industry associations. One of the important roles of these industry associations, within this context, is to make industrial and commercial life more responsible. Industry associations become, as such, "mediating institutions" between the state and the individual and are therefore well placed to

⁸ Industry corporations are also working with public interest groups such as the Internet Education Foundation (<http://www.neted.org>) and America Links Up (<http://www.americalinksup.org>) to further consumer choice in content

promote social responsibility and shared ethical practices among its members ("the industry"). This way of thinking about industry associations - as normative institutions - stands in contrast to how many economists or political scientists think about industry associations and their potential for self-regulation. Analytical models such as the public choice theory with its rent seeking⁹ language teaches us that associations of all kinds, including industry associations, rarely independently of coercion, establish behavioural norms for their members but to serve their private needs. One might prefer to think that industry associations not only serve private interests, but are also motivated by ideals, principles, and values (Rees/Cunningham 1997: 373).¹⁰ In the end, however, the motivation is irrelevant. Associations embody contrary tendencies – primarily the push of self-serving economic (or political) interests, but modified to some extent by the pull of moral aspirations. Indeed, these moral aspirations may have an economic basis. This emergence of a social role for industry associations corresponds to a notable shift in power from the provident State to privatised and multinational enterprise, concomitant with a waning influence of governments and third party organisations on market behaviour. This is especially relevant for the Internet with its increasing globalisation of activity, decentralised architecture and growing networks of enterprises that operate across national boundaries in an array of contractual, equity and joint venture arrangements. In this environment many companies are facing pressure to be accountable even in the absence of explicit state command for non-financial benchmarks in what has been termed the "triple bottom line", a reference to economic, social and environmental performance¹¹.

Self-regulation has proven to work best where there is a degree of coincidence between the self-interest of the industry, and the wider public interest (Cunningham/Grabosky/Sinclair 1998: 53). For instance, it is in the interests of both the Internet Service Providers and the general public to adopt new filtering mechanisms that protect users from offensive material and generate growing confidence. In the advertising industry, self-regulation has voluntarily emerged as the suppliers have perceived the benefit to be obtained from acquiring public credibility for their products and from creating an image of professional responsibility (Boddewyn 1991: 27). Such situations are referred to as "win-win". Where a substantial gap exists between the public interest and the private

selection alternatives.

⁹ Rent Seeking can be defined as the actions and decisions of political actors that result in wealth transfers which reduce the economic well-being of society (Tollison 1982).

¹⁰ Important to mention is that the authors however agree that short-termism is one of the central challenges facing industry self-regulation.

¹¹ The "triple bottom line" concept has received criticism for its potential to compromise three disparate forms of value on one balance sheet (Mayhew 1998).

interest of the industry, it would be naïve to rely upon an industry association taking steps voluntarily in the public interest unless there is some external pressure to do so (the carrot and stick rationale). This may come from a variety of sources, the most important of which include the threat of direct government intervention (enforced self-regulation), broader concerns to maintain credibility and legitimacy (and as a result commercial gain), and the market itself.

Other Industries

While structures of self-regulation vary across industries, its evolution on the Internet will share important common structural elements with other histories. The analysis we have made has its echoes in the work of J. J. Boddewyn, who, in his classic study of self-regulation in the advertising industry found substantial support for a set of clearly relevant hypotheses concerning the effectiveness of such bodies (Boddewyn 1988). For example, he concluded that the existence of an industry-wide decision-making system (such as a capstone trade association) increases the probability of effective industry self-regulation. Industry self-regulation is more effective when it involves all interrelated levels. Just as a scheme that included only advertisers was strengthened if it included distribution systems (such as television networks), a self-regulatory system for the Internet would be strengthened if it included a range of content providers as well as service providers. He also found that the development and effectiveness of an industry self-regulatory system are enhanced by government threat and oversight. The corollary for an Internet context involves, as an example, monitoring and pressure of bodies such as the European Commission or national legislatures on the private sector to take productive action.

It was his view that the strength and effectiveness of an industry self-regulatory system is a function of its essentiality and non-substitutability. Put differently, self-regulation is most effective when, for reasons of practicality, technology and ideology, there is a coherent preference for self-regulation to government action. Further, the existence and effectiveness of industry self-regulation is not measured by formal rules alone, but also by cultural factors. The transnational character of self-regulation and the experience, in each state, of the relationship between government and business are examples of such potential influences.

Other “Boddewyn hypotheses ” include the idea that industry self-regulation is more likely in those situations where self policing can increase the overall demand for the industry’s product and many of the participants. States that encourage self-regulation must convince industry that effective implementation, by enhancing consumer credibility and reducing the threat of costly government

regulation, is self-benefiting. Industry self-regulation is more likely in those situations where the externally imposed costs from not undertaking such self-regulation would be greater than the cost of undertaking such self-regulation. This conclusion recognises the careful calibration that enters the decision to model collective self-regulation. It also suggests that, in a transnational sphere, the calibration of costs in one national context may be different from that in another.

Finally, the creation and improvement of an industry self-regulatory system are precipitated by the threat of governmental regulation. For all of the criticism of “jawboning” or other modes of implying government intervention, the dialogue between government and industry is central to key structures of self-regulation. Also, encouragement and support of industry self-regulation as an instrument of public policy is more likely when the limits of government intervention have become apparent. This may be true, from the outset, in the area of content regulation where free speech and similar concerns underscore the limited role for the state.

The Internet

In the case of the Internet, the very decentralised nature of the enterprise and the deregulatory ethic that pervades it makes defining who is the self (object of self-regulation or who is included in its ambit) especially difficult. In many discussions, governments have failed to recognise that the Internet industry is not monolithic and that there is no single "industry" that speaks for the whole of the Internet. Self-regulatory solutions are probably more appropriately developed on a sector-by-sector basis, on a timetable that fits the needs of that industry sector, and with due recognition and balancing of the extent of the perceived problem (risk of harm) against the risk of regulatory intervention (risk of diminished benefits) (Gidari 1998).

The fact that the Internet is relatively young and still booming also means that in many cases industries do not have a history of effective co-operative action (e.g. creation of industry associations in EU member states). An interesting example of such co-operation is the EuroISPA, the pan-European association of the Internet services providers associations of some EU Member States (<http://www.euroispa.org/members.html>). The association was established when a number of such ISP associations signed the EuroISPA Memorandum of Understanding on 6 August 1997 in Brussels. On 10 September 1997 the signatories to the MOU met again and signed the agreement that formed EuroISPA EEIG, thereby creating the largest association of ISPs in the world. The purposes listed as rationales behind the creation of EuroISPA are: "First, to protect and promote the interests of Europe as a whole within the global Internet, securing for Europe a premier position in

the key industry of the new Millennium. Secondly, to help deliver the benefits of this new technology of liberation and empowerment to individuals, while at the same time meeting the legitimate concerns of parents and others responsible for the weaker members of society. Thirdly, to encourage the development of a free and open telecommunications market, something of great benefit to society as a whole but essential to the healthy development of the Internet. And finally, to promote the interests of our members and provide common services to them where these cannot be had elsewhere". These purposes also highlight the important role of industry associations in the negotiations and bargaining with Governments within a framework of co-regulation or enforced self-regulation.¹²

Competitive Self-Regulation

The multi-sectoral nature of many Internet services will also mean that a wide variety of self-regulating communities or mediating institutions can be expected to come into existence, and even within one given sector competing self-regulatory regimes may emerge. As Ogus has described: "competition of this kind is inherent in systems of private ordering: suppliers compete to attract consumers by the quality (as well as the price) of their products and services. Quality is, to some extent at least, a consequence of standards and other forms of control imposed internally by the management of a firm. The standards may reflect general regulatory requirements but more often they are voluntary, representing the firm's response to assumed consumer demand and, in some cases, incorporating industry-wide practices. To signal to consumers the relationship between standards and quality, some form of voluntary accreditation or certification can be used. Suppliers who aim at different quality standards, and have difficulty in communicating that fact to consumers, will have an incentive to establish a rival certification system" (Ogus 1997). When it comes to providing parental control mechanisms such as filtering and rating software - as described in the chapter by Balkin and Noveck - competition may occur (at the third layer) between white and

¹² In an important contribution to the literature, Ayres and Braithwaite developed their model of "enforced self regulation". Under this model, a public agency negotiates with individual firms regulations that are particularized to each firm, with the threat of an imposition of less tailored standards if it fails to cooperate. While the firm may thus formulate the rules, they are enforced by the public agency. The advantages are clear: as with other privately ordered systems, the rules are tailored to match the firm's circumstances and are less costly to adapt; there are incentives to identify least-cost solutions, which should encourage regulatory innovation; and firms would be more committed to the rules than if imposed externally. Moreover, the very fact of individualization avoids the monopoly problem. On the other hand, the administrative costs would be high. This suggests that, for such a regime to be cost-effective, the firm must be large and the activity to be regulated must be one in which efficiency requires significantly differentiated standards (Braithwaite 1982).

blacklist filters, ancillary rating systems, and redemptive lists maintained by third-party raters. It is important to note in this content that third party raters¹³ usually provide a commercial service which can be combined with the underlying self-regulatory mechanism. The general policy implication of this analysis might be that where the public interest arguments for the state delegating its regulatory powers are strong, a variety of options for users should be stimulated.

There are, nevertheless, potential problems with these solutions. Users - more precisely adults and children - must be able to assess the quality of services provided by the competing options; otherwise there will be a "race to the bottom", with significant welfare costs. To remedy this problem, public and/or private institutional intervention may be desirable that lays down minimum quality standards that the self-regulatory regimes must presumptively satisfy. Such intervention would act as a proxy for insufficiently informed consumers (Ogus 1995). Also efforts to improve general media literacy need to be made. Hence the importance to develop awareness schemes to promote the best use of parental control systems¹³.

Secondly, there must be few significant externalities arising from self-regulation. Regulation has its externalities, and so too does self-regulation. In the area of speech, the external impact of regulation is often carefully measured because state regulation may be "overinclusive," precluding speech practices that are not injurious and might otherwise take place. In the field of regulating indecency on television or the Internet, for example, some courts are concerned that regulation reduces the speech available to adults to that which is suitable for children. In *Butler v. Michigan*, 352 U.S. 380 (1957), the Supreme Court recognised the adverse impact on adults of state laws seeking to benefit children, and, since then, the external consequences of such otherwise beneficial regulation is awarded constitutional significance. Self-regulation inevitably requires the imposition of rules that affect third parties.

There is an ambiguity built in to the very term of "self-regulation." Self-regulation implies, in the first instance, the exercise by firms within the relevant sector of a discipline over their own actions. On the other hand, it also sometimes suggests the exercise of power by firms over the actions of others, where it is they who are regulating rather than the government itself. As an example, one can say that it is self-regulation, in the first meaning of the term, if broadcasters agree that they shall not program material, before a watershed hour, that is potentially harmful to minors. But it may be self-regulation, in the second meaning of the term, if Internet Service Providers agree

¹³ GetNetWise.org is such a scheme recently launched in the US by an industry co-alition including America-OnlineAOL, Microsoft-Group, Yahoo!, and groups like the National Center for Missing and Exploited Childrenre and

to block material that is pornographic or obscene. [The limited technical effectiveness of blocking material on the Internet is discussed in an upcoming publication by Professor Sieber “Verantwortlichkeit im Internet – Technische Grundlagen und medienrechtliche Regelungen” Beck Verlag, 1999 \(“Responsibility on the Internet – Technical Basis and Media Law”\)](#)

Self and Individual Empowerment

There is an increasing social demand for breadth in the definition of "self" for self-regulation. If the function of self-regulation is to minimise harmful and illegal conduct on the Internet (particularly as it affects young people), then in this view, it must become more, rather than less extensive. Albert Gidari, Executive Director of ILPF has stated that, often, the "self" in self-regulation too narrowly focuses on the business sector alone. This narrow conception of self-regulation places too much of the burden on industry to solve the legal and policy issues and fails to recognise individual users of Internet services and other participants as "independent Internet stakeholders and possible administrators" in a larger self-regulatory regime.

One technique is to authorise or require industry to enforce norms against all Internet users. Another increasingly common approach is what is called “individual empowerment”. Individual choice is celebrated in the very nature of the Internet where an individual self-determines what sites to visit, what content to view, and whether to do so anonymously or with the necessary identification to complete a transaction. In response to strong consumer demands, technological tools have been and are being developed to protect against inadvertent exposure to undesired content. In addition, technological complexity is giving way to pre-set preferences; information glut and disorganisation are being replaced by navigation tools, and third-party services that organise, rate or filter according to user instructions. Virtual communities of like-minded individuals form and re-form in an ever-expanding web of information-sharing connections. To be sure, not all individuals have or will achieve complete control over all aspects of electronic transactions. Therefore businesses, alert to consumer preferences, (will have to) respond to these demands by adopting social responsible practices. It is because of these external consequences that the question of the democratic source or legitimisation of self-regulatory activities arises. The power of Internet Service Providers to self-regulate becomes a matter of significant political activity specifically because that self-regulation changes the architecture of communication within society.

Industrial Morality or Social Responsibility

The establishment of norms of behaviour is one of the most complex aspects, theoretically and practically, of collective-self-regulation. To "socialise" industrial life and business activities, an industry association often establishes a normative framework (e.g. enshrined in a code of conduct) for its members. Some may call this "industrial morality," but, to build on an aphorism, this morality may be to altruism what military music is to its civilian equivalent. Still, the articulation of norms, or processes that alter norms, is the basis of many self-regulatory activities with public interest objectives. How such social responsibility comes about is complex, given the wide variety of industries involved, but some common features may be listed (Rees/Cunningham 1997: 376-380).

An industrial morality is a form of moral discourse capable of challenging conventional industry practices ("this is the way we always do business"). Social responsibility provides a basis for shared understanding that can question, guide and set limits around economic considerations by giving a voice to other considerations of what is important for the industry, the consumers, and society such as protection of minors within the setting of the Internet. Self-regulation takes advantage of society's institutional pluralism to moderate the logic of one kind of institution (most notably, the market) by looking at it from the standpoint of another, in this case the parent or the guardian.

An industrial stance on behavioural issues is a product of conscious deliberation. It is the product of collective industry reflection where industry officials question their customary ways of doing business, weigh the alternatives, and think through the consequences of their choices, including the economic impact of certain courses on their collective well-being. Social responsibility recognises multiple values and commitments. An industry association, by developing its norms or establishing norms for third parties (like users of the Internet), asks member companies to resist the single-minded pursuit of any objective, including profits. It asks them to become morally self-aware institutions capable of responsibly balancing economic self-interest with other values. An industrial morality is critical, as it presumes that any existing pattern of industrial conduct is subject to criticism and reconstruction in light of reflection and inquiry. An industrial morality creates a normative framework that defines and upholds a special organisational competence. For members of Internet service provider associations, it is the institutional capacity to promote information flow and access without offending large parts of its users. Social responsibility carries an expectation of obedience. This is not to say that an industrial morality is self-executing,

but rather that great importance is attached to consent in the formation of an industry code of practice. An industrial morality provides a legitimate account of the industry's activities to the public. This is especially important for the Internet industry. Evolving and growing public concern with content freely available to everyone capable of accessing the Internet, forces the Internet industry to develop an industry morality. When an industry's very existence is in question, there is a need for industry to make sense of its relationship to the norms and expectations that exist within its social environment. Hence the importance for the Internet industry to question its scope of responsibility.

Descriptions of the nature of norms on the Internet as self-generated are, however, too simple. The Internet, from the beginning, was a government-sponsored enterprise. In its early, happily chaotic period, the evolution of customs, free of government interference, proceeded apace. Custom, here as elsewhere, became the foundation for law, not necessarily a substitute for it. Industry sought the extension or freezing of this moment of the seemingly autonomous generation of norms. But it was governments from whom this extension of a customary or “unregulated” approach was sought. And it was easy to cloak a policy decision in the altruistic garment of law or regulation avoidance. The US position, and the position of others, on a moratorium on taxation of transactions on the Internet, or the policy against the imposition of other export-import duties, are examples of affirmative policy masquerading as a preference for self-generation of law. Essentially, these questions go to the nature of regulation or how norms are developed by a self-regulatory body. In the case of the Internet, norms are encouraged not through establishing an “industry morality” by the industry alone. The stubborn, dramatic and unfinished process of establishing a rating and labelling schemes is an excellent example of how norms develop through what might politely be called a “conversation” between industry and government. —Among the key questions are whether, and in what circumstances, such rating and labelling efforts suffice to minimise the call for absolute content standards as difficult as they may be to enforce. —A combination of techniques and processes—codes of conduct, rating and labelling and—hotlines and watersheds—may together serve as a way of melding industry conscience with industrial and social needs. The point is that while industry self-regulatory entities do a great deal of work in norm formation, that work must be perceived against a background of potential state coercion.

Institutionalising Social Responsibility and SRA

In its “collective form,” self-regulation is sometimes a deliberate delegation of the state's

law-making powers to an agency, the membership of which wholly or mainly comprises representatives of the industries or individuals whose activities are being regulated. Self-regulatory agencies can also be seen as a delegation of individual and user interests to a private body because of its specific expertise and knowledge. The "self" here can be institutionalised into (separate) self-regulatory agencies (SRA) (or in some cases cartels) that combine the governmental function of regulation -and in some cases enforcement- with the institutional and often legal structure and interests of a private body. They may impose conditions of membership (e.g. solely members of the collective or including outsiders) and expulsion and their own discipline. On the other hand, these self-regulation bodies may only articulate and foster norms, facilitating their adoption without enforcing them. Either way self-regulatory agencies play an important role, acting as intermediaries, linking different parts of society (Black 1996). So, despite the so-called disintermediation or the removal of intermediaries from the industry value chain (Negroponte 1996) as a result of the specific architecture of the Internet, the creation of SRA's may lead to a re-intermediation of the industry.

These self-regulatory agencies have the delicate task of helping to define norms, bringing them to public notice, and creating a sense of "industrial morality." One of the key tasks of an SRA might be to ensure accountability of its members through monitoring or enforcement of standards. One of the principal mechanisms to reach accountability is transparency. There are good grounds to believe that the effectiveness of self-regulation depends on the system's ability to produce and promulgate two kinds of information: (1) about the normative standards the industry has set for itself alone or by agreement; and (2) the performance of member companies in terms of those standards. The first step of public transparency is the public announcement of the principles and practices that the industry presumptively accepts as a guide to its role and also as a basis for evaluating and criticising performance. The next critical step is the development of an information system for collecting data on the progress of member companies in implementing the industry codes or practices. The process usually divides into two parts: (1) reporting by the members and (2) collecting and analysing of the data by the SRA. The third and final step in achieving transparency is the monitoring of performance. Building transparency into the social structure of the industry by those categories sets the stage for a "theatre of external judgement", and as transparency increases so does the likelihood of being called to account for one's industrial conduct (Rees/Cunningham 1997: 383-385).

Reaching accountability and social responsibility is thus an important task of every self-

regulatory body. In carrying out its duties, the (self) regulatory body must, if it is to have any credibility, be seen as having reached its decisions and conducted its activities in an independent manner. This independence is especially important within the communications sector, given the role of media within citizen participation and democracy. Independence is virtually never absolute or complete, but the legal architecture of the body can be reassuring. Guarantees for independence include criteria such as institutional stability (as ensured in its constitution), the appointments system, the composition of the body, the disqualification conditions, the links established between government and industry and its financial and organisational autonomy (Robillard 1995).

"Audited self-regulation", is a US technique that illustrates the relational aspect of self-regulatory independence¹⁴. The conditions used are: "first, the private entity to which self-regulatory authority is granted must have both the expertise and motivation to perform the delegated task. Second, the government agency staff must possess the expertise to "audit" the self-regulatory activity, which includes independent plenary authority to enforce rules or to review decisions of the delegated authority. Third, the statute must consist of relatively narrow rules related output-based standards. ... Finally, the agency's and delegated authority's decision must observe rules for notice, hearing, impartiality, and written records of proceedings and decisions" (Michael 1995: 192). These rules for monitoring would apply to audits by self-regulatory bodies themselves, as well as to those of government auditors.

There are risks of regulatory capture when regulatory agencies become so closely associated with their subject of regulation that it becomes impossible to discern a divergence of interests; at such corporatist moments, the public interest, supposed to be protected by the regulator, may readily be compromised. Such risks may reasonably be heightened in a self-regulatory situation, where the regulators are drawn from and answerable to the industry concerned (Feintuck 1999: 141). Thus transparency, always a prerequisite for accountability as already highlighted, may be of particular significance in relation to self regulatory agencies, given their close relationship with those subject to their rules.

Other issues that arise: the duty or privilege of the SRA to co-operate with government, by, for example, disclosing abuses of a self-regulatory standard to government agencies; the extent to which there is any role for an official or quasi-official agency to have in reviewing or monitoring the performance of SRA and whether the SRA is clothed with any governmental or governmental-like

¹⁴ This term refers to the delegation of power to implement laws or agency regulations to a nongovernmental entity where the federal agency is involved in verifying the soundness of rules, checking compliance, and spot-checking the

powers of enforcement.

2.2. Government and third party involvement

The particular rhetorical relationship between government and the self-regulatory body is most important when considering structure. There is a difference if self-regulation is a consequence of government threat (enforced self-regulation) or a consequence of a civic culture in which the government co-operates with industry (voluntary self-regulation). Self-regulation cannot totally replace government regulation entirely in the media and communications related sectors (Federal Government Germany 1999). The state retains ultimate responsibility for protecting the public interest. This does not mean that the state must directly be involved in the activities of self-regulatory agencies but an interconnection will likely be needed to take sufficient account of compelling public interest considerations. If this interplay is to be a path to better regulatory policy in the Internet field then several points of broader relevance need to be made.

In general, one can identify four types of relationships with the state where the differences among them are delicate but significant: mandated self-regulation, in which the industry is virtually required by the government to formulate and enforce norms within a framework defined by the government. The development of a rating system for the V-Chip in the US falls within one of the first three depending on how one views the process (McDowell/Maitland 1998).; sanctioned self-regulation, in which the collective group itself formulates the regulation, which is then subjected to government approval; coerced (or enforced) self-regulation, in which the industry itself formulates and imposes regulation but in response to threats by the government that if it does not the government will impose statutory regulation. (the creation of the Press Complaints Commission in the UK); and voluntary self-regulation, where there is no active state involvement.

The possibilities can also be considered on two spectra, depicting degrees of autonomy from government and legal force respectively. Rules can be private to firms, groups or organisations at one extreme, to those approved by a government minister or some independent public authority at the other; in between, representatives of the public interest may participate in, but not conclusively determine, the decision-making. Rules may be formally binding, with non-compliance leading to public law or private law sanctions; codes of practice which presumptively apply unless an alleged offender can show that some alternative conduct was capable of meeting the regulatory goals

accuracy of information supplied to it (Michael 1995).

satisfactorily; norms, the breach of which leads to non-legal sanctions, such as ostracism; or standards, with which compliance is purely voluntary.

In determining how to structure the symbiosis between the self-regulating entity and the state, a number of questions can be asked: Was the entity generated from within the industry or as a consequence of government action? Are the broad standards administered by the entity developed by the government or by the entity itself? Who appoints the members of any administering board? Does the board or entity or the industry require state intervention to protect them from liability? Does a consumer have a right of review within the self-regulatory process? Does a consumer have a right of review in the state's judicial system or other processes for review? Is there a public body that periodically reviews the work of the self-regulating entity? Does the industry act through a self-regulating board, or does self-regulation mean that each firm has some responsibility that they are privileged or required to exercise because of industrial consensus? If there is an entity, does it have enforcement powers (is it enforcement when an ISP removes content from a server?) Is there a duty or privilege of the entity (board or company) to co-operate with the state's law enforcement agencies (for example to monitor and then provide information of potential violation of a law)? Is the process of norm-refinement (what constitutes violence for improper material) wholly within the self-regulatory sector and if not how is it divided)?

These questions are part of a taxonomy of self-regulation that is often overlooked. It is rare, as we have emphasized, that a self-regulatory body has (in terms of these questions) no relationship to the state. It is often the case - and this is certainly true in the Internet context - that the generation of self-regulation has its foundation in the possibility or fear of government regulation. In some states, the process of generating self-regulation is a co-operative effort, a suggestion by the state that self-regulation would be a more effective approach than the increase in the definition of illegal conduct by the state itself. In some states, self-regulation figures as a defensive response to a threat, either from political bodies or the public sphere. Self-regulation becomes that body of action, by the industry itself, which can prevent the imposition of more extensive, more costly, more intrusive regulation by government. Self-regulatory entities that develop as a consequence of threat may have different cultures than those that develop as a consequence of negotiation and encouragement. Moreover, for some it seems unlikely that they would perform well in the absence of continuing government oversight and the threat of direct intervention. On the surface, autonomy, where self-regulation is a response to threat, could be defensive, less co-operative, less committed to a common goal. Self-regulation that results from a more positive relationship between state and

industry might be more flexible, lead to greater working together, and have more of a spirit of shared experimentation.

Much clearer elements of autonomy are involved in who establishes the standards that are administered by the self-regulatory entity. In the arena of content control, one of the perceived virtues (though not unalloyed) of self-regulation, is the capacity of users to establish their own standards and not be governed by one standard developed by the government. ~~One might deem a self-regulatory body further removed from the government more capable of articulating standards and administering them that would not be so open for state regulation.~~ However, the more engrafted with state power the self-regulatory body may be through setting certain standards in the architecture of speech, for instance; the more it is appropriate to scrutinise the nature of its approach to affecting content so as to insure that private does not take the place of public censorship.

Whatever standards are self-created by the private regulating entity, it still may have an administrative role with respect to standards that have been enacted as a positive prohibition by the state. In the Internet context, all states have laws that prohibit certain kinds of speech in whatever medium. These may include speech that incites violence, or speech that endangers national security in highly specified ways. While administration or enforcement of these prohibitions rests, usually, with the state, they can be administered by the self-regulating entity as well. More difficult is a description of speech regulating techniques that are different from those established by the state.

In almost every national setting concerning the Internet, self-regulation with respect to content will, increasingly, have one significant relationship to the state: a pact in which the service provider is willing to undertake affirmative actions to remove potentially illegal harmful material from its servers, but requires immunity from the state for such actions. It is possible that contractual arrangements will entitle service providers (or others similarly situated) to remove what are deemed offensive materials, or cut off access to servers, or discontinue use by particular individuals or entities. But contract protection alone -and even that implicates the state -may not be sufficient if the self-regulating entity is to play the wider role that seems to be demanded of it. The state is being called upon to ensure that, within a particular ambit of action, the service provider will not be open to lawsuit, even if the removal of material proves to be erroneous or exceeding what constitutes illegality within the society. Such a provision was included as a so-called Good Samaritan law in the 1996 Telecommunications Act in the United States. It finds a curious mirror in a recent addition to the US Copyright Act (Section 512(c)) designed to deal with potential copyright infringement in the digital world. That law authorises the service provider expeditiously to remove or disable access to

material that is claimed to be infringing a third party copyright. The statute provides very specific circumstances under which a service provider is notified as to potentially infringing activity. In Section 512(g), the statute provides that a service provider "shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing."

Self-regulating entities will require this kind of immunity from liability if they are called upon to take down material thought to be harmful, especially if they do so expeditiously, without the kind of due process that would be required if the state were engaged in exercising content controls. Even more so than in cases of disputed copyright infringement, there will undoubtedly be differences of opinion of what harmful content should be removed (either because of contract or because of codes of conduct or because of alleged violation of statute).

The state will be implicated in yet another way, this time to ensure greater freedom for the service providers. Increasingly, self-regulating entities require state assurance of a safe harbour. Again, the Communications Decency Act, even though struck down in part, is a model of what may come. In that statute, service providers could escape responsibility for delivering certain material to minors or displaying it to minors if they complied with specific techniques that were surrogates for actual determination of minimum age of addressee.¹⁵ These included, for example, the use of credit cards (47 USCA 223(e)(5)(B)) Two elements are important here. Certain elements of self-regulation must be protected through state law. More significant, however, state law may itself rely on the self-regulatory mechanism to introduce comparable or acceptable mechanisms to determine what constitutes such things as a safe harbour. Three more elements of state involvement can be mentioned.

Self-regulatory mechanisms may be privileged in terms of their enforcement. We have already dealt with this in the analogy to the privileging of private entities to eliminate potential copyright infringers. More may be anticipated in terms of empowering the self-regulator. Second, the state may require, or at least excuse, actions, that otherwise might be violations of user privacy

¹⁵ 47 USCA 223(e)(5) It is a defense to a prosecution under subsection (a)(1)(B) or (d), or under subsection (a)(2) with respect to the use of a facility for an activity under subsection (a)(1)(B) that a person--(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or (B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

or contractual rights, by notifying law enforcement of possible harms that exist through particular uses of the Internet. Indeed, self-regulation might involve monitoring content, and a concomitant protected responsibility to evaluate and to report. Much of this is dealt with in Professor Sieber's chapter in this book. Finally, the state might require public review of the activities of the self-regulating entity and determine the composition of the reviewing mechanism. An interesting example of this was the announcement in September 1998, by the UK's Department of Trade and Industry (DTI) and the Home Office to carry out a review of the Internet Watch Foundation (Department of Trade and Industry 1999).

Third Parties

The state is however not the only party that might develop co-regulatory arrangements with the industry. Sometimes, there may also be a possibility of harnessing third parties or "outsiders" to act as surrogate regulators; monitoring or policing the code as a complement or alternative to governmental involvement. It is possible to argue that self-regulation is rarely effective or legitimate without such involvement. The most obvious third parties with an interest in playing this role are sectoral interest groups such as consumer associations, trade unions or NGOs generally. Moreover with the individual empowerment made possible through the technologies of the Internet, the consumer him/herself may play an important role as co-regulator. A distinction between four major types of outside participants can be made: public members (also called "independents"), consumer representatives, experts and professionals. In practice, most self regulatory systems use some mixture of all four types. Government agencies and officials can be considered as a fifth category of outsiders. They do not officially participate within a self regulatory agency but informally guide, monitor and even threaten them (as discussed above) (Boddewyn 1988: 52).

This contribution of third parties or the so-called "co-opted" self regulation may be through their direct involvement in administration and auditing of the code itself (with often greater credibility of the self regulatory scheme as a result), or in their capacity as potential victims of code malpractice, in taking direct action against firms that breach the self regulatory program. One major consequence of harnessing the self-interest of consumers through self-regulatory programs is that there is far less need for direct involvement of government. A major role of governments in these circumstances may be that of facilitator or broker (ensuring the effective involvement of appropriate third parties) rather than that of direct participant.

Non-member controls: summary

Self regulators may thus be subject to government and non-member controls in a host of ways (Baldwin/Cave 1999):

- statutory prescriptions and objectives;
- rules that are drafted by or approved by other bodies or ministries;
- ministerial guidelines or criteria for consideration by the self-regulator;
- parliamentary oversight of the delegated legislation that guides the self-regulator;
- departmental purse strings and the influence that these provide;
- agency oversight;
- informal influences from government that are exerted in the shadow of threatened state regulation;
- judicial review;
- complaints and grievance-handling mechanism (e.g. ombudsmen);
- reporting and publication requirements laid down by government or parliament.

2.3. Codes of Conduct

One form of industry self-regulation is the development of an industry-wide normative framework, a set of industrial principles and practices that defines right conduct as it spells out the industry's public commitment to moral restraint and aspiration. An evolving framework in many cases, it is usually drafted in very general terms at the outset because trust, co-operation, and technical consensus necessary for a more detailed agreement is lacking; but as co-operation and consensus grows, it is usual for more detailed norms to follow. Studies of the prevalence and contents of codes of conduct have shown that their use to define a socially responsible and ethical environment, and their effective implementation, must be as part of a learning process that requires inculcation, reinforcement and measurement (National Consumer Council 1986). One of the conclusions made by the Internet Law and Policy Forum was that "the history of self-regulatory initiatives proves that snapshot solutions are ineffective. Instead, the basic premise of self-regulation is continuous improvement to meet the needs of the particular business in the most efficient manner (with "needs" encompassing company growth and consumer demand as well as the prevention and detection of unlawful or liability-producing conduct). For example, third-party or internal audits are proven self-regulatory tools. Successful audits build on prior audit results and

become management tools for future improved performance. The process is iterative and repetitive, resulting in best practices that often are adopted or emulated by others in the same industry to remain competitive." (Gidari 1998).

Codes of conduct are designed to protect an organisation's or industry's public image, and to a certain extent to enhance it, by declaring its moral standards to others. A hazard of industry codes is that while they may be useful and accurate descriptions of the organisational or industrial paradigm, they are likely to be only partially accurate, and even misleading descriptions of actual industry practices (Doig/Wilson 1998: 141). This is simply because the statements of aspiration or strategic intent emanate from a particular stakeholder. (Johnson/Scholes 1997: 218). The question whether the association or body responsible for the code represents all the operators in a sector or only a small percentage of them is, therefore, a crucial one to answer.

There is a related danger of codes. While they appear to make the industry socially responsible and working for the benefit of those who use the services of the industry, the codes may become a means merely to sell the firm to customers and employees. One important criterion for judging the value of a code against this type of "window-dressing" is the degree to which its rules can be enforced. In this context, the strength of the association is crucial in terms of its ability to impose sanctions on its members for non-compliance with the code.

As to the Internet, several ISP associations have now developed or are in the process of developing different codes concerning, among other things, the protection of minors (BIAC/OECD, <http://www.oecd.org/dsti/sti/it/index.htm>). Several secondary reasons suggest, that industry-wide or profession-wide codes--with clearly comprehensive coverage--are more useful instruments of protection than those developed by small groupings of companies within sectors. From the user's point of view, an industry that is fragmented and characterised by several rival associations, each with its own content protection code, is confusing. The co-existence of several different codes creates an overall picture that lacks transparency for the user. Particularly on the Internet offensive or illegal content is passed between different companies of the same sector. Situations can arise where the company evaluating the content is not subject to the same protection code as the company that receives it. This is a source of considerable ambiguity as to the nature of the rules applicable, and it might also render investigation and resolution of complaints from individual users extremely difficult.

The Content of Codes of Conduct

Generally codes¹⁶ developed by the Internet Service Providers tend to focus on:

- co-operation with law enforcement authorities,
- clarification of liability and responsibility issues,
- approaches to privacy and handling personal data,
- investigation of complaints,
- procedures for addressing illegal or harmful content,
- promotion of technological tools to empower users.

As to illegal or harmful content the European Council Recommendation of 24 September 1998 provided an overview of what should be included in such a code (Council of Ministers 1998).

Concerning the protection of minors, codes of conduct should address basic rules:

- on the nature of the information about Internet content to be made available to users, its timing and the form in which it is communicated. The most appropriate occasions should be chosen to communicate such information (sale of technical equipment, conclusion of contracts with user, web sites, etc.).
- for the businesses providing on-line services and for users and suppliers of content. The rules should set out the conditions under which the supply and distribution of content, likely to harm minors, is subject to protection measures such as: a warning page, visual signal or sound signal, descriptive labelling and/or classification of contents, and age-verification systems.
- on the conditions under which, wherever possible, additional tools or services are supplied to users to facilitate parental control, including: - filter software installed and/or activated by the user, and filter options activated, at the end-user's request, by service operators at a higher level (for example, limiting access to predefined sites or offering general access to services).
- on the management of complaints, i.e. on the provision by operators of appropriate management tools and structures to receive complaints without difficulty (through hotlines: telephone, e-mail, fax) and on the introduction of procedures for dealing with complaints (informing content providers, exchanging information between operators, responding to complaints, etc.).

Several additional observations are relevant. Whatever the content of such codes, transparency is a crucial element. When drafting codes, language should be plain and offer concrete examples to

¹⁶ See Appendix for some examples

illustrate various provisions. A distinction may be made among principles, codes, and what might be called guidelines and recommendations, a distinction that relates to the strength of obligations imposed on industry. General principles are close to incontrovertible axioms that all members of the industry association should accept as self evident. Codes refer to explicit rules, whose violation is most likely to trigger some admonition or disciplining. Guidelines and recommendations are of a less binding nature because the problems are novel, fluid and/or hard to clearly circumscribe so that precise (or hard) rules are not possible. Honesty, decency, fair trading and the like are typically amenable to such looser treatment. In the field of advertising, self-regulatory systems are increasingly issuing recommendations rather than firm rules for fear that language that is too explicit increases the danger of voluntary codes will be transformed into laws and regulation. Appropriate rules for appeal and mediation procedures should also be included in a code of conduct.

Effectiveness of Codes of Conduct

The Working Group on the Protection of Individuals with Regard to the Processing of Personal Data of the European Commission (DG-XV) recently analysed the effectiveness of industry self-regulation, with results that can be adapted to content self-regulation (European Commission 1998). The four functional criteria they suggest for judging the effectiveness of a self-regulatory code are: level of compliance, support to users, impartiality of the arbiter and appropriate redress.

Level of compliance The level of compliance is likely to depend on the degree of awareness of the code's content among members, on the steps taken to ensure transparency of the code to consumers, on the existence of a system of external verification (such as a requirement for an audit of compliance at regular intervals) and, perhaps most crucially, on the nature and enforcement of the sanction in cases of non-compliance.

When examining the types of sanction in place, it is important to distinguish between a "remedial" sanction which simply requires a service provider, in case of non-compliance, to change its practices so as to bring them into line with the code, and a sanction which goes further by actually punishing the provider for its failure to comply. According to the Working Group, it

is this second category of "punitive" sanction which has the greatest effect on future behaviour by providing a strong incentive to comply. The absence of genuinely dissuasive and punitive sanctions is seen as a major weakness in a code. [A-It can be argued, however, that a](#) rigorous system of external verification (such as a public or private authority competent to intervene in case of non compliance with the code, or a compulsory requirement for external public audit at regular intervals) can provide strong incentives for a high level of overall compliance.

Important questions listed by the Working Group are: what efforts does the representative body make to ensure that its members are aware of the code? Does the representative body require evidence from its members that they have put the provisions of the code into practice? Is such evidence provided by the member company itself or does it come from an external source (such as an accredited auditor) and at what intervals is it provided? Does the representative body investigate alleged or suspected breaches of the code? Is compliance with the code a condition of membership of the representative body or is compliance purely "voluntary"? Where a member has been shown to breach the code, what forms of disciplinary sanction are available to the representative body (expulsion or other) ? Is it possible for an individual or company to continue working in the particular profession or industry even after expulsion from the representative body? Is compliance with the code enforceable in other ways, for example by way of the courts or a specialist tribunal?

Support and help to users A key requirement of an adequate protection system is that an individual faced with a problem is not left alone, but is given some institutional support. This institutional support should ideally be impartial, independent and equipped with the necessary powers to evaluate any complaint. Where the problem concerns illegal content on the Internet, there should be, at least, a preliminary evaluative inquiry, though such complaints must, eventually be channelled to the proper law enforcement authorities. Details of this process are addressed in the chapters on hotlines [and](#) on law enforcement. Relevant questions for self-regulation in this regard are: is there a system in place allowing for evaluation of complaints from users? How are users made aware of this system and of actions taken in individual cases? Are there any costs involved for the user?

Impartiality of the arbiter The impartiality of the arbiter or adjudicator in any alleged breach of a code is key. -Clearly such a person or body must be independent in relation to the service provider. This in itself may not be sufficient to ensure impartiality. Possibly, the arbiter should be independent from the profession or sector concerned, the reason being that fellow members of a profession or sector have a commonality of interests with the actor alleged to have breached the

code or might otherwise be subject to a conflict of interest.

Appropriate Redress If the self-regulatory code is shown to have been breached, not only should a remedy be available to the user, but that remedy must be appropriate. Sanctions have a dual function: to deter the offender (and thus encourage compliance with rules) and to repair or cure a breach of [the](#) rules. –The repair function seems to be more important to the Working Party. Additional questions would therefore include: how is it possible to verify that a member who has been shown to contravene the code has changed his practices and put the problem right? Will users deem that the sanctions have led to a situation in which the code is observed more fully?

Current Examples and Internet Practices

It is difficult to assess the current status of self-regulatory practices in a comparative way. Often, self-regulatory efforts are non-public and not reported. They take different forms in different areas of the world. There are flaws in survey techniques as categories for description may vary between the surveying entity and the businesses or governments being surveyed. As the Internet changes, as social needs are defined, self-regulatory practices change and change rapidly. Some examples may, however, be given to demonstrate the institution of self-regulatory practices especially if it involved the creation of industry associations and the designing of codes of conduct.

Europe The majority of efforts to self-regulate and consequently to draft codes of conduct for the Internet in Europe came in 1997 when there was an explosion of activity. To protect their interests vis-à-vis the intentions of government, working parties or industry associations were established then in Belgium (ISPA), France (AFPI), Ireland (ISPA), Italy (@IIP), and in Germany (ICTF/FSM). All have since drafted codes of conduct (see appendix) including references to mechanisms (rating and filtering) and rules to protect minors. Some of them also created a complaints mechanism or hotline (e.g. Newswatch (G), Meldpunt (NL), IWF (UK), AFA (Fr)) These efforts were preceded by the earlier organisation of self-regulation of the Internet in both the Netherlands (NLIP est. 1995) and in the UK (ISPA est. 1995 and Internet Watch Foundation est. 1996). These forerunners have ~~since~~ been followed [more recently](#) by efforts in Spain (Anprotel), Denmark (FIL), Austria (ISPA) and Finland (ISPA). Further, Internet service providers in [the](#) Greece are in the process of setting up an official association -and -Sweden's leading Internet service providers are also in the process of holding discussions to create a framework for self-regulation in their country. Some of these efforts have also been combined across Europe through the creation of

Euro-ISPA, the pan-European association of the Internet services providers associations of the countries of the European Union. Other Pan-European efforts include INCORE (Internet Content Rating for Europe), funded by the European Commission, to create a forum to examine questions of content rating and subsequent filtering and -INHOPE -(Internet Hotline Providers in Europe).

~~-Abroad international effort to develop, implement and manage an internationally acceptable voluntary self-rating system was recently created. Among the founding members of the Internet Content Rating Association (ICRA) (Internet Content Ratings Alliance)¹⁷ was created by among others AOL, British Telecommunications plc (BT), Cable & Wireless, Demon Internet, IBM, Internet Watch Foundation, the Electronic Network Consortium (Japan), EuroISPA, Bertelsmann Foundation and Microsoft and is as such transatlantic, T-Online and the Bertelsmann Foundation¹⁸.~~

North America There has been a great deal of activity in the US and Canada. In November 1995, the Task Force on Internet Use of the Information Technology Association of America issued a report on "Internet, Free Speech and Industry Self-Regulation". It concluded by stating that ITAA "believes a reasonable and rational middle ground exists that allows the Internet to continue to flourish, while at the same time giving parents and families the tools necessary to negotiate safely on the information superhighway. This approach recognizes the need for industry self-regulation rather than legislative intervention. ITAA intends to continue pursuing a balanced approach, what it views as the better alternative".

This has been followed by several high level summits on Internet content and Child Protection and at the state level several ISP associations have been created. Examples are as follows: in Texas the non-profit Texas Internet Service Providers Association (TISPA) was founded in 1996. According to TISPA's bylaws, initiatives will be developed "to disseminate legislative, educational and other useful information and to inspire Members to further inform themselves in the practical and ethical issues of the Internet industry" (<http://www.tispa.org/bylaws.htm>). State law requires all Texas Internet Service Providers to link to blocking and filtering software sites. In 1997, during the 75th Regular Session of the Texas

¹⁷ ICRA's mission is to develop, implement and manage an internationally acceptable voluntary self-rating system which provides Internet users world wide with the choice to limit access to content they consider harmful, especially to children. ICRA has received the RSAC assets including the RSACi system that provides consumers with information about the level of nudity, sex, language, and violence in Web sites.

¹⁸ ICRA's mission is to develop, implement and manage an internationally acceptable voluntary self-rating system which provides Internet users world wide with the choice to limit access to content they consider harmful, especially to children. ICRA has received the RSAC assets including the RSACi system that provides consumers with

Legislature, House Bill 1300 (HB 1300) was passed. HB 1300 requires Internet Service Providers to make a link available on their first world wide web page (home page) which leads to Internet "censorware" software, also known as 'automatic' blocking and screening software. The Florida Internet Service Providers Association was founded in May, 1996 "to facilitate discussion and educate the public about the importance of the Internet industry". A Code of Conduct was drafted that reflects general principles of good conduct (http://www.fispa.org/fispa_code.html).

In Canada the Canadian Association of Internet Providers (CAIP), created in 1996, has issued a voluntary Code of Conduct with an accompanying commentary (<http://www.caip.ca/caipcode.htm>).

Australia On the 21st April 1999, the Minister for Communications, Information Technology and the Arts introduced Internet legislation, known as the Broadcasting Services Amendment (Online Services) Bill 1999. Among the listed provisions, the Australian Broadcasting Authority (ABA) will be given powers to issue notices to service providers aimed at preventing access to prohibited material which is subject to a complaint if it is hosted in Australia. If the material is sourced overseas, the ABA is authorized to take reasonable steps to prevent access if technically feasible and commercially viable. Such "reasonable steps" are to be detailed in an industry Code of Practice to be developed in consultation with the ABA. There are several associations at the state level such as the South Australian Internet Association, the ACT Internet Association, the Tasmanian Internet Association and the Western Australian Internet Association. At a national level there is the Internet Industry Association (incorporating the Australian Internet Alliance, and the Internet Industry Association of Australia).

Some examples may be given from *Asia* In Japan, the Electronic Network Consortium has developed its General Ethical Guideline for Running Online Services in 1996 (<http://www.nmda.or.jp/enc/guideline.html>). Similar guidelines, "Codes Of Practice For Internet Service Providers" were approved by the Telecom Services Association on January 30, 1998 (http://www.telesa.or.jp/e_guide/e_guido1.html). To protect young people and public morals, a Practice Statement was developed that recommends guidelines for members of the Hong Kong Internet Service Providers Association (HKISPA) (<http://www.hkisp.org.hk/>) to follow in their provision of services insofar as the regulation of obscene and indecent material transmitted on the Internet is concerned. Finally, in Singapore, in exercise of the powers conferred by section 18 of

the Singapore Broadcasting Authority Act, the Singapore Broadcasting Authority issued, with effect from November 1, 1997, the Internet Code of Practice (<http://www.sba.gov.sg/netreg/code.htm>).

Part 3. Conclusions & Recommendations: Systematic Self Regulation as a Foundation

Given the competing societal interests in control of content on the Internet, meaningful and effective self-regulation is preferable to the exclusive exercise of government authority. ~~Self-regulation contain~~ has a greater capacity to adapt rapidly to quickening technical progress and to the transnational development of the new communications medium. ~~In addition to flexibility, self regulation presents the additional~~ benefits of greater efficiency, increased incentives for compliance, and reduced cost. A carefully structured program of self-regulation, often developed in cooperation with government, is harmonious with the new technology, mirroring the Internet itself as a global, essentially private and decentralised network of communication.

Effective self-regulation requires active consumer and citizen consultation based upon shared responsibility at all stages of development and implementation. Without user involvement, a self-regulatory mechanism will not accurately reflect user needs, will not be effective in delivering the standards it promotes, and will fail to create confidence. Moreover, the effectiveness of self-regulation and its enforcement will depend largely on the full collaboration and commitment among all industry players. Self-regulation can then yield a responsive, acceptable and systematic solution to current concerns.

The development of an effective self regulatory regime for the Internet includes the formation of multiple, carefully considered, comprehensive and complementary ~~structures and the creation of important mechanisms~~ to achieve public interest objectives. The establishment of self-regulatory mechanisms that have a reservoir of social acceptance will, in general, be the product of public input and ~~useful~~ cooperation among Internet Service and Content Providers, ~~other elements of a~~ self-regulatory ~~mechanisms nationally and internationally~~ and state bodies.

Self Regulatory Agencies (SRA), should be brought into being ~~national and across borders~~ for the creation, promulgation and enforcement of self-generated codes. SRAs should stimulate public confidence by ensuring accountability, monitoring of members and enforcing standards.

Codes of conduct should be adopted to ensure that Internet content and service providers act in accord with principles of social responsibility. These codes should meet community concerns and industry needs and operate as an accountability system that guarantees a high level of credibility and quality. To be

effective, these codes of conducts should be the product of and enforced by the self-regulatory industry entities themselves, though often in collaboration with government. Because of the transnational nature of Internet communications, coordinated activity among these agencies is an essential element of self-regulation.

There should be comprehensive use of rating and filtering technology and a mobilization of content producers worldwide to empower users of the Internet to make more effective choices about program content. Such technology is especially necessary for content directed to children or content that might, in the absence of mechanisms, enter homes without the capacity of guardians to exercise their judgment. Such a comprehensive system requires citizen content response and complaints systems, such as Hotlines, that add to credibility.

In implementing codes, several additional principles are important. Effective self-regulation is not possible without support processes of law making and regulation. In addition, ~~Public education~~ is essential to increase awareness of the means to filter and block content, to present complaints for effective redress and to obtain the level of compliance that is promised by the industry. Finally, techniques must be found to measure the effectiveness of self-regulatory measures and to determine what national and trans-national measures—if any—are necessary to compensate for their deficiencies. Codes of conduct should ~~should~~ delineate both the standards for problematic content which they are attempting to enforce and the mechanisms through which this enforcement will occur, including provisions for cooperation with end users as well as public authorities. Industry-wide codes are more useful instruments of protection than those developed by small groupings of companies within sectors. They are more comprehensive and transparent and reduce confusion among users. ~~In order to make codes more efficient and to create internationally consistent minimum rules with respect to illegal content, these codes should be incorporated into contracts between Internet providers and their clients, in agreements among providers themselves, and in agreements between providers and self-regulatory bodies or agencies.~~

For self regulation to ensure public confidence, standards for protection of minors must be clear and effective. ~~These standards should be developed by the SRA's themselves, if possible (or if not, by public bodies).~~ They should be transparent, and accepted by government as the mode for proceeding for the protection of youth. There are necessary, state-authorized conditions for self-regulation. ~~In rare cases,~~ ISPs must have the protected capacity to exclude potentially violative ICPs from ~~publicly available their~~ servers. And, in carefully specified instances, ISPs must have the protected capacity or "safe harbour" of ~~handling and~~ sharing information with law enforcement authorities, but the circumstances for such sharing should be

circumscribed and the specific circumstances for sharing should be fully disclosed.

Bibliography

Aalders, Marcus/ Ton Wilthagen 1997: Moving Beyond Command-and-Control: Reflexivity in the Regulation of Occupational Safety and Health and the Environment. *Law & Policy*, 19, pp. 415-443

Ayres, Ian/ John Braithwaite (1992): Responsive Regulation: Transcending the Deregulation Debate. Oxford, Oxford University Press.

Baldwin, Robert/Christopher McCrudden (1987): Regulation and Public Law. London: Weidenfeld and Nicolson.

Baldwin, Robert/Martin Cave (1999): Understanding Regulation. Oxford: Oxford University Press, 1999.

Birks, Peter (1997): Privacy and Loyalty. Oxford: Clarendon Press.

Black, J. (1996): Constitutionalising Self-Regulation. *The Modern Law Review*, 59, pp. 24-56.

Boddewyn, J.J. (1991): The Case of Self Regulation. NY: IAA.

Boddewyn, J.J. (1998): Advertising Self-Regulation and Outside Participation: A Multinational Comparison. New York: Quorum.

Braithwaite, John (1982): Enforced Self Regulation: A New Strategy for Corporate Crime. *Michigan Law Review*, 80, pp. 1466-1507.

Braithwaite, John (1993): Responsive Regulation in Australia. In: Peter Grabosky/John Braithwaite (eds.): Regulation and Australia's Future. Canberra: Australian Institute of Criminology, p. 91.

Breyer, Stephen (1982): Regulation and its Reform. Cambridge, Massachusetts: Harvard University Press.

Brohmer, Jurgen/J. Ukrow (1999): Die Selbstkontrolle im Medienbereich in Europa. Eine rechtsvergleichende Untersuchung. Saarbrücken: EMR.

Campbell, Angela J. (1999): Self-Regulation and the Media, 51 *Fed. Comm. L.J.* 551

Cunningham, Neil/Peter Grabosky/Peter Sinclair (1998): Smart regulation – Designing Environmental Policy. Oxford: Clarendon Press.

Delacourt, J. (1997): The International Impact of Internet Regulation. *Harvard International Law Journal*, 38, p. 207.

Doig, A./J. Wilson (1998): The Effectiveness of Codes of Conduct. *Business Ethics*, 7, p. 141.

Doyle, C. (1997): Self Regulation and Statutory Regulation. *Business Strategy Review*, 8 (3), pp. 35-42.

Feintuck, M. (1999): Media Regulation, Public Interest and the Law. Edinburgh: Edinburgh University Press.

Gidari, A. (1998): Observations on the State of Self-Regulation of the Internet. The Ministerial Conference of The OECD A Borderless World: Realising the Potential for Global Electronic Commerce. Ottawa, Canada.

Goldsmith, Jack L. (1998): Against Cyberanarchy. *University of Chicago Law Review*, 65, p. 1199.

Harden, I./N. Lewis (1986): The Noble Lie: The British Constitution and the Rule of Law. London: Hutchinson.

Hawkins, K./B.M. Hutter (1993): The Response of Business to Social Regulation in England and Wales: An Enforcement Perspective. *Law & Policy*, 15, p. 199.

Hoffmann-Riem, Wolfgang (1996): Regulating Media: The Licensing and Supervision of Broadcasting in Six Countries. New York: Guildford Press.

Huysse, L./S. Parmentier (1990): Decoding Codes: The Dialogue between Consumers and Suppliers through Codes of Conduct in the European Community. *Journal of Consumer Policy*, 13, p. 260.

Johnson, Gerry/Kevin Scholes (1997): Exploring Corporate Strategy. Prentice Hall: New York.

Katsh, M.E. (1996): Dispute Resolution In Cyberspace. *Connecticut Law Review*, 28, p. 953.

Mayhew, N. (1998): Trouble with the triple bottom line. *Financial Times*, 10 Aug. 1998.

McDowell, Stephen D./Carleen Maitland, (1998): Developing Television Ratings in Canada and the United States: the Perils and Promises of Self-Regulation. In: Monroe E. Price (ed.): The V-Chip Debate. New York: LEA.

Michael, Douglas C. (1995): Federal Agency Use of Audited Self-Regulation as a Regulatory Technique. *Administrative Law Review*, 47, p. 171.

Negroponte, Nicholas (1996): Being Digital. New York: Vintage Books.

Ogus, A. (1995): Rethinking Self-Regulation. *Oxford Journal of Legal Studies*, 15, pp. 97 –108.

Ogus, A. (1997): Self-Regulation. In: B. Bouckaert/G. De Geest (eds.): Encyclopedia of Law and Economics.

Oreja, Marcelino (1999): Seminar on Self-regulation in the Media (jointly organised by the German Presidency of the European Union and the European Commission). Saarbrücken (speech).

Page, A.C. (1987): Financial Services: The Self-Regulatory Alternative? In: R. Baldwin/ C. McCrudden (ed.): Regulation and Public Law. London: Weidenfeld and Nicolson, pp. 298 – 321.

Pitofsky, Robert (1998): Self-Regulation and Anti-trust, <http://www.ftc.gov/OPA/1998/9802/SE;FREG.HTM> (visited July 14, 1999).

Prosser, T. (1998): Law and the Regulators. Oxford: Clarendon Press.

Rees, J. (1988): Reforming the Workplace, A Study of Self Regulation in Occupational Safety. Philadelphia: University of Pennsylvania Press.

Rees, J./N. Cunningham (1997): Industry Self-Regulation: An Institutional Perspective. *Law & Policy*, 19 (4), p. 364.

Schmitter, P.C. (1985): Neo-Corporatism and the State. In: Wyn Grant (ed.): The Political Economy of Corporatism. London: Macmillan, pp. 32-62.

Sinclair, D. (1997): Self Regulation Versus Command and Control? Beyond False Dichotomies. *Law & Policy*, 19 (4), p. 529.

Tollison, Robert D. (1982): Rent Seeking: A Survey. *Kyklos*, 35, pp. 575-602.

Ukrow, J., (1999): Self Regulation in the Media Sector and European Community Law. Saarbrücken: EMR.

Wacks, R. (1997): Privacy in Cyberspace: Personal Information, Free Speech and the Internet. In: P. Birks (ed.): Privacy and Loyalty. Oxford: Clarendon Press, pp. 93 – 112.

Internet Resources

America Links Up <http://www.americalinksup.org> (visited July 14, 1999).

America Online, <http://www.aol.com> (visited July 14, 1999).

BIAC/OECD Internet Forum on Content Self Regulation, <http://www.oecd.org/dsti/sti/it/index.htm> (July 14, 1999).

Canadian Association of Internet Providers, <http://www.caip.ca/caipcode.htm> (visited July 14, 1999).

Cyber Rights & Cyber Liberties, <http://www.cyber-rights.org/isps/somm-dec.htm> (visited July 14, 1999).

Electronic Network Consortium, <http://www.nmda.or.jp/enc/guideline.html> (visited July 14, 1999).

European Advertising Standards Alliance, <http://www.easa-alliance.org/> (visited July 14, 1999).

European ISP Association, <http://www.euroispa.org> (visited July 14, 1999).

Florida ISP Association, http://www.fispa.org/fispa_code.html (visited July 14, 1999).

Global Business Dialogue on Electronic Commerce, <http://www.gbde.org/gbde.html> (visited July 14, 1999).

Hong Kong ISP Association, <http://www.hkispa.org.hk/> (visited July 14, 1999).

International Telemedia Association, <http://www.telemedia-ita.org/> (visited July 14, 1999).

Internet Education Foundation, <http://www.neted.org> (visited July 14, 1999).

Safe Surfin', <http://www.safesurfin.com/> (visited July 14, 1999).

Singapore Broadcasting Authority, <http://www.sba.gov.sg/netreg/code.html> (visited July 14, 1999).

Telecom Services Association, http://www.telesa.or.jp/e_guide/e_guido1.html (visited July 14, 1999).

Texas ISP Association, <http://www.tispa.org/bylaws.htm> (visited July 14, 1999).

Primary Sources

Council of Ministers (1998): Recommendation 98/560/EC on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity. Official Journal L 270 07/10/1998 p. 0048.

Department of Trade and Industry in the Home Office (1999): Review of the Internet Watch Foundation. London: KPMG and Denton Hall, <http://www.kpmgiwf.org/> (visited July 14, 1999).

European Commission (1996): Green Paper on the protection of minors and human dignity. COM (96) 483, final.

European Commission (1997a): Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation: Towards an Information Society Approach. COM(97)623. <http://www.ispo.cec.be/convergencegp/97623en.doc> (visited July 14, 1999).

European Commission (1997b): Follow-up to the Green Paper on the protection of minors and human dignity in audiovisual and information services. COM (97) 570, final. http://europa.eu.int/comm/dg10/avpolicy/new_srv/com1v-en.htm (visited July 14, 1999).

European Commission (1998): Working Document: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country? Adopted by the Working Party on 14 January 1998, DG XV D/5057/97.

Federal Government Commissioner for Cultural Affairs and the Media (1999): Conclusions of the Experts' Seminar on Media Self Regulation. Saarbrücken.

Internet Law and Policy Forum (1998): Bibliography on Self-regulation on the Internet, <http://www.ilpf.org/selfreg/selfreg2.htm> (visited July 14, 1999).

Ministry of Consumer Affairs (1997): Market Self Regulation and Codes of Practice. A Policy Paper By The Ministry Of Consumer Affairs. New Zealand.

National Consumer Council (1986): Self Regulation of Business and the Professions: An NCC Background Paper. London.

National Telecommunications Information Administration (1997): Privacy and Self Regulation in the Information Age, Introduction.

OECD (1997a): Approaches to Content on the Internet. DSTI/ICCP (97), p. 10.

OECD (1997b): Co-operative Approaches to Regulation. Public Management Occasional Papers No 18.

OECD (1998): Working Party on the Information Economy: The Economics of Self-Regulation on the Internet. DSTI/ICCP/IE (98) 7, p. 6.

Cases

Butler v. Michigan, 352 U.S. 380 (1957).

Reno v. ACLU, 117 S.Ct. 2329 (1997).

Reno v. ACLU, 31 F.Supp 2d 473 (1999).

APPENDIX – CODES OF CONDUCT

I. AFA - Association des Fournisseurs d'Accès et de Services Internet

STANDARDS AND PRACTICES

January 1998

The AFA is the French Internet Services Providers Association.

Internet professionals should be distinguished according to their activity i.e., principally: access provider, content provider, hosting provider, infrastructure provider.

The AFA also stresses the distinction between the access provider's activity, which involves providing users with access to contents which the provider has no part in, and the on-line services activity which involves providing users with access to contents placed on line by the on-line services company or by third parties which are independent as far as practices are concerned.

In conformity with its public information remit, the AFA wants to stipulate the framework within which its members carry on their business activities, describe their practices, and certify to the confidence Users (subscribers or occasional users) place in them.

To this end, the AFA has formulated a draft of the standards and practices of its members.

I. THE PRINCIPLES COMMON TO AFA MEMBERS

1) Netiquette

The communities set up via Internet, in distribution lists or newsgroups, have drawn up rules of conduct generically known as "netiquette".

Non compliance with these rules may result in the exclusion of the user contravening them, even though such rules may only be tacit.

In general, netiquette enjoins Internet users to exercise moderation in expressing ideas - as far as both form and content are concerned - to be polite and respectful of others, the purpose being to harmoniously make use of the communication possibilities provided by Internet, without cluttering up the network or inconveniencing its users.

AFA members are also concerned to limit the practice of sending out unsolicited electronic mail on a large scale ("spam"). To this end, they are putting in place computer tools designed to detect spams and reduce their transmission.

AFA members are favourable to the principles of netiquette, in as far as they aim to protect freedom of expression and the correct management of the network.

For this reason, AFA members inform their Users of the existence of these informal rules in their general subscription conditions or when accessing the service.

2) Confidentiality

2.1 Data throughput

In the framework of the services they provide, AFA members have made means of accessing the Internet network available to their Users.

In carrying on this business activity, they consider they have neither the right nor the means of exercising control over the mass of information conveyed over their network web. They act as a carrier (relayer) in the same way as a Post Office which knows the address and size of packages without knowing their contents.

2.2 Electronic mail

AFA members respect the confidentiality of private correspondence.

Mail is usually erased from the servers on which they are saved before being delivered to the User's computer, as soon as they are received by the latter or after a given time.

2.3 Identification items for access to the service

All the items allowing Users to identify themselves and log onto the service are personal and confidential. All use of identification items falls under the entire responsibility of Users.

2.4 User identification

AFA members are not permitted to communicate nominative information concerning their Users, outside cases authorized by the law.

In conformity with the legal provisions in force, AFA members may, at the behest of police or judicial authorities, be required to reveal the identity of one of their Users.

3) Responsibility

Users express themselves freely on Internet. They are responsible for their behaviour.

AFA members stress that, as the data circulating on the Internet may be subject to regulations governing use or be protected by ownership rights, Users are each responsible for their own use of such data.

4) Protection of minors

A wide variety of information is available on the Internet.

As a result,

- subscriptions are refused to minors unless otherwise authorized by someone with parental authority,
- AFA members offer their Users solutions allowing them filter contents on their microcomputers (by PICS or Cyberpatrol for example), even before the corresponding contents are sent over the network.

II. THE DAILY EXPERIENCE OF AFA MEMBERS

While certain AFA members produce and place on line some information on their own behalf, most of the information available on the Internet is produced and placed on line by third parties, whether individuals or entities, which may or may not be Users of the services of AFA members.

1) Contents produced and placed on line by some AFA members

AFA members are responsible for what they produce and place on line on their own behalf.

In accordance with the current conventions on the Internet, AFA members consider that addresses of Internet sites may be freely mentioned in editorials.

As this involves on-line debates proposed and coordinated by AFA members, the latter resort to moderators responsible for monitoring discussions, each participant being responsible for its remarks.

2) Contents produced and placed on line by AFA Users: Personal Pages

AFA members, which are not responsible for the contents placed on line by their Users, check that the latter comply with their General Conditions.

In practice, Personal Pages, which can at any time be modified by their author, cannot reasonably be subject, as far as AFA members are concerned, to a systematic, exhaustive check of their content, any rights which may be attached to them, or any links they may have with other sites.

AFA members have the possibility of detecting contents which are manifestly illegal.

To date, three main means can be used:

- criticisms from users,
- monitoring of pages most frequently consulted (and directly linked sites),
- automatic detection of suspicious words (use of so-called crawler software).

However, the effectiveness of software detection is reduced as soon as those responsible for the monitored sites have knowledge of the "suspicious" words looked for by the access provider's computer program.

The monitoring of pages most frequently consulted and the following up of criticism on the part of users make it possible to detect most manifestly illegal contents, although not all.

3) Contents produced and placed on line by third parties

3.1 On the network

By definition, AFA members are not the authors or the publishers of the contents produced and placed on line by third parties.

The fact that it is possible to retrieve the image of often demanded contents from the memories of the Proxies of an access provider corresponds to a routing characteristic specific to Internet.

3.2 In discussion groups ("Newsgroups")

This involves unmoderated public discussion forums.

Access providers have no means of preventing the setting up of discussion groups, which they do not initiate. That being the case, they can take no action until after illegal discussion groups have appeared.

AFA members can prevent the distribution of discussion groups which do not comply with their General Conditions of Use, or by means of a legal injunction.

In practice, AFA members suspend the distribution of discussion groups:

- either by filtering the titles of newsgroups,
- or when the existence of such newsgroups is brought to their knowledge.

Filtered groups may, however, still be available to be consulted through other access providers in France or abroad.

3.3 By direct messaging (IRC)

As with discussion groups, access providers have no way of preventing the setting up and broadcasting of discussion channels or topics they are not the initiators of, and which are by nature volatile.

As previously and under the same conditions, they can take no action until after illegal discussion topics have appeared.

III. RELATIONS WITH USERS: FRAMEWORK OF CONFIDENCE

Although a few legal actions have been brought to the forefront of the scene, AFA members, in the daily exercise of their profession, manage to deal with most complaints on good terms with their Users.

If users are confronted on the network with contents which are illegal or which offend them, they can easily refer this to the access provider.

An access provider, which is a member of the AFA, will quickly assess the complaint in view of the contract entered into with the User in question and will act on a case by case basis:

- if the content placed on line or the attitude of the User in question is contrary to its General Conditions of Use, the access provider takes action requesting the User to change its attitude or the content in question,
- if such a request proves to be insufficient, it gives notice to the User to modify its attitude or its content, and if necessary may delete the contents at fault or terminate the subscription.

The setting up of a Consultative Committee responsible for dealing with questions of relations between Internet users would make it possible to formalize what is now current practice of AFA members.

II. Code of Conduct of the Association

"Freiwillige

Selbstkontrolle Multimedia-Diensteanbieter e.V."

Preamble

The Association for the Voluntary Self-Monitoring of Multimedia Service Providers ("Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V."; FSM in short) wishes to make its contribution toward strengthening the freedoms of service providers and protecting the valid interests of users and the general public, in particular against race discrimination and the glorification of violence, and to act on the basis of self-responsibility in order to strengthen protection for youth. Any form of censure will be rejected.

The Association for the Voluntary Self-Monitoring of Multimedia Service Providers wants to encourage service providers to join in order to make them abide by the principles of the Code of Conduct and punish any violations of this code.

The Association for the Voluntary Self-Monitoring of Multimedia Service Providers respects the freedom of expression inherent in individual communication within the services offered, and the basic rights of users to freedom of information. At the same time, the Association for the Voluntary Self-Monitoring of Multimedia Service Providers respects the basic right to freedom of the media (press) and the basic right to economic freedom (provision of commercial services).

The Association for the Voluntary Self-Monitoring of Multimedia Service Providers shall not unreasonably encroach upon any third party's rights or interfere with other countries' legal systems.

The Association for the Voluntary Self-Monitoring of Multimedia Service Providers, by providing information regarding its own work, applying technical protection mechanisms as preventive measures against any misuse, and establishing an information and contact office, strives to communicate the idea of responsible use of the services by users and service providers.

The obligations put forth in this Code of Conduct should not and cannot be used as grounds for establishing responsibility to any third parties, nor assist in the substantiation of such responsibility. The contact office procedure shall not preclude legal recourse.

The Association for the Voluntary Self-Monitoring of Multimedia Service Providers will cooperate with other voluntary self-monitoring bodies - also at European and international level - in order to cover the global range of services, as well as the international nature of the networks and service providers.

I. Code of Conduct

1. Scope

The Code of Conduct shall bind the members of the "Association for the Voluntary Self-Monitoring of Multimedia Service Providers. (FSM)". If an association becomes a member, then the companies it represents shall also be bound by the Code of Conduct, provided they have submitted a commitment to this effect.

The principles established in the Code of Conduct shall not represent any legal grounds for liability.

This Code of Conduct shall apply to the extent to which those who provide services and those who switch services (media services/ teleservices and similar services) are responsible for the content of the services pursuant to the currently applicable statutory regulations of the Federal Republic of Germany.

This Code of Conduct has the goal of preventing the provision of impermissible services pursuant to section 2 and ensuring compliance with standards pursuant to sections 3, 4 and 5 hereof.

The Code of Conduct does not cover any violations of legal provisions under laws on advertising and promotion, data protection, consumer protection, or competition.

The tasks of other existing self-monitoring bodies as well as the self-monitoring measures of individual members of the Association regarding the services shall remain unaffected.

2. Principles of conduct - Impermissible content

The members of the Association for the Voluntary Self-Monitoring of Multimedia Service Providers shall take all actions, within the scope of legally determined responsibility and to the extent actually and legally possible and reasonable, to ensure that content which is unlawful or impermissible, in particular pursuant to

- a) §130 of the StGB1 (Incitement to hatred and violence against segments of the population (or minority groups) or publishing insults against them in such a manner as to endanger the peace or to expose them to scorn or contempt);
- b) §130a of the StGB (Incitement to commit crimes);
- c) §131 of the StGB (Depiction of acts of violence, instigation to racial hatred);
- d) §86 of the StGB (Dissemination of propaganda material of unconstitutional organizations);
- e) §87 of the StGB (Treasonable conduct as an agent for sabotage purposes);
- f) §184 (3) of the StGB (Dissemination of pornographic publications),
is neither provided nor switched for use.

3. Principles of conduct - Impairment of the well-being of children/ young persons

(1) The members of the Association for the Voluntary Self-Monitoring of Multimedia Service Providers shall take all actions, within the scope of legally determined responsibility and to the extent actually and legally possible and reasonable, to ensure that content which is unlawful or impermissible, in particular pursuant to

- a) § 8, Nos. 5 and 6 of the MdStV2;
- b) § 184 (1) of the StGB (Dissemination of pornographic publications),
is neither provided nor switched for use.

(2) The members of the Association for the Voluntary Self-Monitoring of Multimedia Service Providers shall take preventive measures, within the scope of legally determined responsibility and to the extent actually and legally possible and reasonable, to ensure that content which may impair the physical, mental, or spiritual well-being of children or young persons is neither provided nor switched for use, unless

- a) care is taken that children and young persons do not become aware of the services under normal circumstances, or
- b) users are offered technical arrangements which allow them to block the services according to their specific, individual needs.

The service providers shall inform users of such options.

Membership of the Association for the Voluntary Self-Monitoring of Multimedia Service Providers covers the obligations pursuant to § 7 of the GjS3 and § 8 (4) of the Mediendienste-Staatsvertrag4

4. Principles of conduct - Contents in style of journalistic reporting

If the services provided by members of the Association for the Voluntary Self-Monitoring of Multimedia Service Providers contain content in the style of journalistic reporting as stipulated in the Mediendienste-Staatsvertrag, the

members of the Association shall ensure, within the scope of legally determined responsibility, that

- a) content intended for reporting purposes, and containing information services, complies with generally accepted journalistic principles;
- b) reports about topical news items are verified by the provider before publication with the appropriate care regarding content, origin and truthfulness;
- c) editorial comment is clearly distinguished from news reports, and the author of editorial comment is identified as such;
- d) a statement is made as to the representativeness of surveys carried out by members of the Association and quoted in their services.

In defining generally accepted journalistic principles for the purposes of this Code of Conduct, reference may be made, where appropriate, to the Code of Conduct of the German Press Council in the applicable version.

5. Provider identification

Members of the Association for the Voluntary Self-Monitoring of Multimedia Service Providers that act as content providers shall ensure that the statutory regulations for identification of providers are complied with. Members that merely act as switching agents shall ensure, as far as reasonably possible, that the content providers comply with such regulations.

II. Sanctions

6. Measures

a) Should the relevant bodies of the Association for Voluntary Self-Monitoring of Multimedia Service Providers, on the basis of the Grievance Rules adopted by the Association, determine that a breach of the Code of Conduct has been committed, the following sanctions can be implemented:

- Notification with demand to take remedial action, or
- expression of disapproval, or
- reprimand.

Should the relevant bodies of the Association for Voluntary Self-Monitoring of Multimedia Service Providers decide to implement sanctions against a member of the Association due to a breach of the Code of Conduct, the member undertakes to comply with said sanctions. The member shall take action to ensure that the breach is not repeated.

b) Notifications with demands for remedial action and expressions of disapproval shall remain unpublished; reprimands shall be made public in paraphrased form.

Reprimand shall be published by the provider in the service concerned for the period of one month. If the service is terminated before the reprimand is given, the reprimand shall be published in a comparable place for the period of one month.

c) Should a member, despite repeated demands, fail to take remedial action against a breach of the Code of Conduct or fail repeatedly to comply with sanctions - although this is actually and legally possible and reasonable - the member may be excluded from membership of the Association for Voluntary Self-Monitoring of Multimedia Service Providers.

The relevant bodies of the Association for Voluntary Self-Monitoring of Multimedia Service Providers shall not be bound by instructions.

III. Services offered by non-members

7. Provision and switching of services by non-members

(1) The Association for the Voluntary Self-Monitoring of Multimedia Service Providers may also deal with content that is offered, provided for use, or technically switched by non-members.

(2) Any complaint about such services shall also be decided on the basis of the provisions of this Code of Conduct and handled in accordance with the Grievance Rules.

(3) The Association for the Voluntary Self-Monitoring of Multimedia Service Providers shall inform the non-member of its decision, and shall encourage the non-member to take remedial action, if appropriate.

(4) Neither the decision nor any demand for remedial action shall be published.

IV. Final provisions

8. Future updates

The members of the Association for the Voluntary Self-Monitoring of Multimedia Service Providers agree to continuously review and revise the Code of Conduct and the catalogue of sanctions on the basis of day-to-day practice.

Cologne, 9 July 1997

1 StGB = Strafgesetzbuch; German Criminal Code

2 MDSStV = Mediendienste-Staatsvertrag; Agreement on Media Services between the Federal Länder in Germany

3 GjS = Gesetz über jugendgefährdende Schriften; Act on Publications Morally Harmful to Young Persons

4 Agreement on Media Services between the Federal Länder in Germany

III. NLIP-KEURMERK

versie 1.0, d.d. 10/12/97

Vooraf:

Het NLIP-keurmerk, dat (incl. NLIP-beeldmerk) alleen en uitsluitend gevoerd mag worden door NLIP-leden, bestaat uit 2 onderdelen.

- Onderdeel I zijn de Algemene leverings- en consumentvoorwaarden van de NLIP, en is gericht op het ondubbelzinnig vastleggen van belangrijke elementen in de relatie provider - particuliere abonnee (aanbieder - consument).
- Onderdeel II beschrijft het minimum service level (de technische kwaliteitseisen) t.b.v. het product Internetaccess voor consumenten.

Het NLIP-Keurmerk (versie 1.0) geldt m.i.v. 1 november 1997, met dien verstande dat voor organisaties die op die datum al lid waren van de NLIP een overgangstermijn geldt van 6 maanden.

Het NLIP-Keurmerk is een dynamisch keurmerk. Het NLIP-keurmerk wordt jaarlijks, in overleg met consumenten- en andere organisaties, geëvalueerd, verbeterd en uitgebreid. Voor 1998 staat uitbreiding gepland met onderdelen voor backbone-providers, voor contentproviders, en voor het product Internetaccess voor bedrijven.

Definities

NLIP:

Vereniging van Nederlandse Internet Providers.

Provider:

Lid van de NLIP, aanbieder van Internetdiensten

Abonnee:

Particuliere consument die diensten van provider afneemt.

Dienst:

De door provider ter beschikking gestelde mogelijkheden berichten, informatie, program ma's en/of gegevens op elektronische wijze op te slaan, te raadplegen, te bewerken en/of te transporteren. De diensten zijn nader omschreven in de overeenkomst.

Overeenkomst:

de afspraken, schriftelijk vastgelegd in een formulier, document of anderszins, op grond waarvan door provider één of meer aansluiting(en) en/of diensten ter beschikking worden gesteld.

NLIP-KEURMERK ONDERDEEL I:

Algemene leverings-/consumentvoorwaarden van de NLIP.

1.1. Briefgeheim

en hanteert het briefgeheim met betrekking tot persoonlijke e-mail.

Provider respecteert

1.2. Privacy

abonnee-bestand niet aan derden ter beschikking
Provider informeert abonnee duidelijk en vooraf m.b.t. welke gegevens aan derden (kunnen) worden doorgegeven. Deze gegevens zijn binnen de organisatie van provi der alleen toegankelijk ten behoeve van de bedrijfsvoering. Geheimhouding / beveiliging. Provider draagt zorg voor een beveiliging als bedoeld in de Wet Persoonsregistraties van alle gegevensverzameling en die mogelijk per soonsgegevens bevatten, voorzover dergelijke verzamelingen in het kader van de uitvoering van de overeenkomst in het systeem van provider alsmede in de door hem in verband

daarmee gehouden administraties aanwezig zijn. De geheimhoudingsplicht geldt tenminste twee jaar na beëindiging van de overeenkomst of zoveel langer krachtens wettelijke regelingen.

I.3. Wet- en regelgeving

Provider en

abonnee houden zich aan de Nederlandse wet- en regelgeving.

I.4. NLIP-klachtenregeling

Provider hanteert de

NLIP-klachtenregeling (zie www.nlip.nl, klachten) voor het ontvangen en afhandelen van klachten.

I.5. NLIP-geschillencommissie

Provider is

aangesloten bij de NLIP-geschillencommissie (zie www.nlip.nl, klachten).

NLIP-KEURMERK ONDERDEEL II:

minimum service level t.b.v. Internetaccess voor consumenten. 1. Kwaliteit van dienstverlening en informatie.

- A. *Informatie.* Op de WWW server van de provider dient de volgende informatie, makkelijk vindbaar, aanwezig te zijn: bedrijfsnaam, inschrijfnummer kamer van koophandel, postadres, fax- en telefoonnummers, openingstijden, functionele emailadressen. Verder dienen de abonnees minimaal te kunnen beschikken over de namen van SMTP-, POP- en evt. newsservers, IP nummers nameservers, inbelnummers.
- B. *Telefonische bereikbaarheid.* Bij 2 x per minuut proberen op het drukste moment van de dag moet in 95% van de gevallen een abonnee binnen 15 minuten een medewerker van de provider aan de lijn krijgen. Als er meerdere nummers (bijvoorbeeld administratie en helpdesk) zijn geldt deze eis voor ieder nummer apart. Telefoonnummers moeten minstens 4 uur per werkdag opengesteld zijn.
- C. *Email en fax.* Email en faxen dienen in 95% van de gevallen binnen 3 werkdagen beantwoord te zijn. Is dat niet mogelijk dan wordt aan de abonnee een ontvangstbevestiging gestuurd met een indicatie wanneer de vraag wordt beantwoord.

2. Kwaliteit van de Internet-services.

- A. *Services.* De provider biedt aan inbellende abonnees, afgezien van het forwarden van IP pakketten van/naar het Internet, minimaal de volgende services: SMTP relay, POP of IMAP mailbox of batched SMTP, DNS.
- B. *Beschikbaarheid.* Alle services zijn, individueel gemeten, 98% van de tijd, gemiddeld per maand, beschikbaar. Onderhoudstermijnen worden geteld als "niet beschikbaar".
- C. *Serversnelheid.* Alle services dienen in 95% van de gevallen binnen 20 seconden te reageren op willekeurig welk commando.
- D. *IP-forwarding.* Geldige IP pakketten met een geldig adres, verstuurd vanaf het Internet naar een abonnee die online is of andersom, worden niet gefilterd en de inhoud wordt niet gewijzigd.

3. Kwaliteit van de Internetverbinding.

- A. *Congestie.* Packetloss mag niet hoger dan 3% zijn. (Bij custom queuing geldt het cijfer van de queue met de hoogste packetloss waar verkeer van abonnee doorheen gaat.)
- B. *Snelheid.* Round-trip (ping) tijden van "snelle" sites mogen niet hoger zijn dan 500 ms (exclusief vertraging modem/ISDN). (Bij custom queuing geldt de tijd van de traagste queue waar verkeer van abonnee doorheen gaat.)
- C. *Doorvoersnelheid intern.* FTP van/naar FTP server van provider dient met een doorvoersnelheid van minstens een derde van de modem/ISDN snelheid te gaan.
- D. *Nameserver.* Antwoordtijden + vertraging interne netwerk mag niet meer dan 100 ms zijn (exclusief vertraging modem/ISDN) voor informatie die zich al in de nameserver cache bevindt.

4. Kwaliteit van de inbelvoorziening.

- A. *Bereikbaarheid.* Op de drukste tijd van de dag dient bij 2 x per minuut proberen in 95% van de gevallen binnen 10 minuten een verbinding tot stand te komen.
- B. *Inbelproblemen.* Als de lijn opgenomen wordt dient in 98% van de gevallen een verbinding opgebouwd te worden die minstens 15 minuten actief en bruikbaar blijft (tenzij de inbeller de verbinding verbreekt).
- C. *Naam.* Een aan een abonnee toegewezen IP adres dient te beschikken over een geldige naam en daarmee corresponderende reversed mapping van het adres.

5. Email

- A. *Ontvangen*. In 99% van de gevallen is een emailbericht binnen 24 uur na het bereiken van een server met een volledige Internetverbinding afgeleverd bij de geadresseerde of is een foutmelding met beschrijving van de reden waarom het bericht niet afgeleverd kon worden teruggestuurd.
- B. *Versturen*. In 99% van de gevallen is een emailbericht binnen 24 uur na het aanbieden aan de SMTP server afgeleverd bij een MX host van het geadresseerde domein of is een foutmelding met beschrijving van de reden waarom het bericht niet afgeleverd kon worden teruggestuurd.
- C. *Grootte*. De maximumgrootte van email-berichten die verstuurd en ontvangen kunnen worden dient minimaal 256 kilobyte te zijn.
- D. *Grootte mailbox*. De mailbox van een abonnee moet minstens een megabyte groot zijn.
- E. *Forwarden*. Nadat een abonnee vertrekt wordt email op diens verzoek nog drie maanden lang naar een nieuw email-adres doorgestuurd, tegen een af te spreken vergoeding.

6. News (indien dat onderdeel uitmaakt van het abonnement).

- A. *Lezen*. 95% van alle postings in NL groepen dient binnen 36 uur op een voor inbellende abonnee toegankelijke newsserver aanwezig te zijn.
- B. *Posten*. In 99% van de gevallen is binnen 12 uur na het posten in een NL groep door een inbeller de betreffende posting aanwezig op minstens twee newsservers buiten het domein van provider.
- C. *Expire*. Articles dienen ten minste drie volle dagen op de server beschikbaar te blijven.

7. Beveiliging.

- A. *Vertrouwelijkheid*. Vertrouwelijke gegevens, zoals gebruikersinformatie, en email, zijn niet door derden te benaderen.
- B. *Software*. De provider houdt zich op de hoogte van alle relevante beveiligingslekken en neemt de nodige maatregelen om "exploits" te weren.
- C. *Backups*. Gebruikersbestanden, incl. e-mail, worden door provider minimaal 1 x per week geback-upped.

8. Voor alle meetbare criteria geldt:

- A. Alle meetwaarden worden regelmatig gemeten en per kwartaal aan de NLIP gemeld, of op de eigen site van provider vermeld. Door onafhankelijke derden zullen onregelmatig- /steekproefsgewijs metingen worden verricht.
- B. Bij afwijkingen die een slechtere prestatie aanduiden wordt door provider direct actie ondernomen ter verbetering van de situatie.

9. Voor alle regels uit onderdeel II geldt dat uitzonderingen mogelijk zijn indien provider aannemelijk kan maken dat:

- A. Het niet voldoen veroorzaakt wordt door een gebeurtenis of partij waar provider geen invloed op of relatie mee heeft, en provider alle maatregelen die redelijkerwijs verwacht mogen worden om deze situatie te voorkomen of te verhelpen genomen heeft (overmacht).
Het niet voldoen geen nadeel voor abonnee oplevert tegenover een situatie waarbij provider wel aan de betreffende minimum-eis voldoet (geen schade).

I

V. Gedragscode ISPA-Belgium. Versie 1.0

Inleiding

Onderhavige gedragscode vindt haar oorsprong in het kader van het economisch belang van de Internet- en telecommunicatie markt. De markt is immers uniek en kent geen voorgaanden. Ze wordt gekenmerkt door hoog technologische nieuwigheden en een wereldwijd, onbegrensd aspect. Gelet op het belang van deze markt voor de economie en de handel, dient elke belemmering van de bedrijvigheid zoveel mogelijk vermeden te worden.

De gedragscode is hiertoe een nuttig instrument. Het zal toelaten bestaande regelgeving niet alleen in het domein van de handel en de economie maar ook op crimineel vlak te interpreteren en te concretiseren naar deze nieuwe bedrijvigheid toe.

1. Preambule

Deze Gedragscode ("Code") regelt het gedrag van de leden van de Internet Service Providers Association ("leden"). De Code is uniform en verplichtend voor alle leden zonder veranderingen of uitzonderingen. Een lid mag bijgevolg niet, op grond van een contract of anderszijds, de toepassing van de Code vermijden of omzeilen. Leden dienen overeen te komen met de geest evenals met de letter van de Code.

De naleving van de Code wijst er op dat de leden handelingen stellen als een Goed Huisvader die Te Goeder Trouw zijn diensten uitvoert. De Code kan dan ook als richtlijn voor de evaluatie van het optreden van de Internet Service Providers (ISP's) gebruikt worden.

2. Algemene Vereisten m.b.t. commercieel handelen

Rechtmatigheid en Oprechtheid

De diensten-, produkten- en promotie materiaal van de leden worden op een rechtmatige en oprechte wijze aangeboden. Leden zullen op geen enkele manier het onwettig handelen op het Internet stimuleren.

Leden zullen zich inspannen om te verzekeren dat hun diensten- en promotiemateriaal niet misleidend zijn door inaccuraatheid, ambigüiteit, overdrijvingen, verzwijgingen of op een andere wijze.

Eerlijke handel

Bij het handel drijven met klanten en andere bedrijven, zullen de leden ten alle tijde op een behoorlijke, eerlijke en redelijke wijze optreden.

De leden zullen hun klanten inlichten over het bestaan van de Code en de klachtenprocedure.

Data-protectie

De persoonlijke gegevens m.b.t. de klanten kunnen door de leden enkel gebruikt worden voor rechtmatige doeleinden. De leden dienen de Wetgeving m.b.t. de bescherming van de persoonlijke levenssfeer te respecteren.

Advertentie, draagwijdte

In geval van publiciteit zullen de leden verzekeren dat de advertenties uitgezonden via radio, televisie, teletekst, fax of op enige ander wijze overeenstemmen met de bepalingen van de wet.

Prijsinformatie

De leden moeten verzekeren dat de prijzen voor hun diensten duidelijk en ondubbelzinnig opgesteld zijn. Voor persoonlijke aansluitingen zijn de prijzen BTW inbegrepen. Indien additionele prijzen betaald dienen te worden, dient dit meegedeeld te worden.

3. Algemene vereisten m.b.t. bestrijding van criminaliteit en externe klachtenprocedure

Internet Service Providers zullen zich naar best vermogen inspannen om onrechtmatige en schadelijke handelingen op het Internet mee te helpen bestrijden. Zij zullen er zich toe verbinden zich terzake op redelijke wijze in te spannen met betrekking tot het legaal gebruik van Internet.

Internet Service Providers zijn echter niet in de technische mogelijkheid om alle informatie verspreid via de Internet-infrastructuur te controleren. Hun taak betreft niet het controleren en/of het regelen van de wijze waarop klanten of derden de Internet diensten invullen of gebruiken. Zij zullen de daartoe bevoegde instanties evenwel onverwijld en onvoorwaardelijk helpen met alle middelen die ter hun beschikking staan:

- a. De Internet Service Providers verbinden zich ertoe hun klanten te identificeren.
- b. De Internet Service Providers zullen een "Acceptable Use Policy" toevoegen aan de standaardvoorwaarden van de overeenkomsten met hun klanten. Hierin wordt een "aanvaardbaar gedrag op het Internet" opgelegd. De Acceptable Use Policy zal aan de Internet Service Provider de mogelijkheid geven de nodige daden te stellen (o.a. schorsing van overeenkomst met klant). Internet Service Providers voorzien een mail-adres waar klachten kunnen geformuleerd worden door iedere derde aangaande onrechtmatige praktijken die via het Internet gebeuren.
- c. De Gerechtelijke Politie richt een Meldpunt (1) op i.v.m. alle activiteiten en informatie die in strijd is met het strafrecht of met de goede zeden o.a. reclame voor diensten van seksuele aard; aanslag op de goede zeden (pedofilie en kinderporno, bestialiteit, sadomasochisme, necrofilie); racisme en xenofobie; ontkenning van de genocide; kwaadwillige provocatie tot het plegen van misdaden en delicten; groeperingen van misdadigers; spelen en loterijen; verdovende middelen en psychotrope stoffen (bijvoorbeeld Internet-sites waar men in België verboden drugs en medicijnen kan bestellen), enz.
- d. Derden, waaronder de Internet Service Providers, zijn in de mogelijkheid activiteiten en informatie verspreid via Internet en in strijd met het strafrecht of de goede zeden zoals hierboven vermeld, mede te delen aan het Meldpunt, zodra zij hiervan expliciet op de hoogte zijn gesteld.
- e. ISPA alsmede de Internet Service Providers verbinden zich ertoe de nodige inspanningen te leveren opdat dit Meldpunt kenbaar gemaakt wordt aan haar cliënteel, o.a. door vermelding hiervan op haar website en door de contractuele voorwaarden.
- f. De communicatie tussen het Meldpunt en de Internet Service Providers zal het voorwerp uitmaken van een apart document dat door de belanghebbenden zal opgesteld worden.
- g. De leden volgen de instructies van de Gerechtelijke Politie.

4. **Interne klachtenprocedure i.g.v. niet conform handelen met de Code door een lid**

De procedure voor het behandelen van de klachten zal verschillen overeenkomstig het initiatief van de klachten. In hoofdzaak zijn er drie verschillende wijzen voor de behandeling van de klachten:

- a. Een klacht wordt geformuleerd door een derde rechtstreeks aan een ISPA lid. Het lid zal de klacht behandelen tot er een bevredigende oplossing is gevonden.
- b. Een klacht wordt geformuleerd door een derde rechtstreeks aan een ISPA lid. Het lid faalt in de behandeling van de klacht. De klager verwijst de klacht naar het Bestuur van ISPA.
- c. Een klacht kan ook rechtstreeks door een derde aan het Bestuur worden geformuleerd.

Eens de klacht verwezen is naar het ISPA Bestuur zal de behandeling verschillen van de aard van de klacht. Het Bestuur bepaalt de aard en inhoud van de klacht en zal overleg plegen met de betrokken leden. Vooreerst de klacht te behandelen kan het Bestuur belanghebbende derden raadplegen. Het Bestuur zal de klachtbehandeling communiceren naar de leden en het lid waartegen een klacht werd ingediend.

Indien een klacht bevestigd wordt door het Bestuur, kan het Bestuur volgens haar eigen discretie de door haar geleden redelijke administratieve kosten bij de behandeling van de klacht terugvorderen.

Het Bestuur zal het lid eerst op informele basis benaderen.

Indien een lid in de mogelijkheid is te reageren op het advies van het Bestuur doch dit onredelijkerwijze weigert, of indien een lid herhaaldelijk schuldig bevonden wordt de Code niet na te leven, kan het Bestuur de klacht registreren als een formele klacht tegen dit lid, desgevallend beslissen het lid te schorsen.

5. **Wijziging van de Code**

ISPA kan stellingen formuleren die betrekking hebben op het Internet gebeuren in België. Deze stellingen kunnen geïncorporeerd worden in de Code. De Code kan gewijzigd worden bij 2/3 van de van stemmen door de leden aanwezig op de Ledenvergadering. ¹ Punt 3 kan slechts van toepassing zijn voor zover een Meldpunt wordt gecreëerd.

V. Il Testo del Codice di Autoregolamentazione

Introduzione

Internet è una rete mondiale in cui tutti i contenuti e i servizi presenti sono accessibili da qualsiasi utente ovunque esso si trovi, senza alcun vincolo di tipo geografico. Questa caratteristica della Rete è estremamente positiva, ma rende difficilmente realizzabile una regolamentazione dei contenuti e dei servizi presenti attraverso una normativa comune, stante le differenze culturali, politiche e normative tra i diversi Paesi.

Internet è un sistema di comunicazione interattivo che, rispetto ai media di massa tradizionali, ha alla base, e come peculiare ricchezza, il coinvolgimento diretto degli utenti nella creazione, oltre che nella fruizione, dei contenuti e dei servizi.

Internet è uno strumento flessibile che permette di comunicare a molteplici livelli e con diverse modalità: si va dal modello della "pubblicazione" a quello dell'interazione pubblica o privata, dallo specifico testuale puro, alla comunicazione multimediale, dalla trasmissione di messaggi a quella di programmi per elaboratore.

In questo flusso di informazioni e atti, che già oggi supera largamente ogni altra forma di comunicazione tradizionale per volume di scambi comunicativi, può nascondersi il comportamento illecito in base a taluni o tutti gli ordinamenti giuridici o il contenuto potenzialmente offensivo per alcune categorie di utenti. E' dunque opportuno che siano prese misure per limitare eventuali effetti dannosi che questi contenuti e comportamenti possono arrecare.

Per questo motivo gli operatori del settore sentono la necessità di adottare un codice di condotta che, in coerenza con le caratteristiche peculiari della rete Internet:

- tenga presente le esperienze internazionali e le soluzioni individuate in tema di autoregolamentazione del settore negli altri paesi - con particolare riferimento agli Stati Membri dell'Unione Europea -, in modo da accrescerne l'efficacia in un contesto necessariamente internazionale;
- si fondi sul diritto alla libertà di espressione e di comunicazione;
- sia studiato in modo da evolversi nel tempo coerentemente con l'elevato tasso di innovazione che caratterizza le tecnologie legate al mondo Internet.

Il presente codice tiene conto tra l'altro delle indicazioni in materia del Consiglio e della Commissione dell'Unione Europea (Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services del 16 ottobre 1996, Risoluzione del Consiglio del 17 febbraio 1997).

Titolo I - Disposizioni preliminari e principi generali

1. Definizioni

Ai fini del

presente Codice valgono le seguenti definizioni:

- Internet (di seguito indicata anche come Rete): insieme di reti di computer interconnessi tra loro tramite linee di telecomunicazione e comunicanti utilizzando protocolli della famiglia TCP/IP.
- TCP/IP: protocollo (linguaggio di comunicazione) utilizzato per la trasmissione dei dati in Internet.
- Infrastrutture: linee di telecomunicazione e apparati necessari al funzionamento della Rete.
- Accesso: connessione alla Rete, necessaria al fine di utilizzarne le risorse.
- Hosting: messa a disposizione di una parte delle risorse di un server al fine di distribuire contenuti o servizi attraverso la Rete.
- Server: computer connesso alla Rete atto alla erogazione di servizi.
- Contenuto: qualsiasi informazione messa a disposizione del pubblico attraverso la Rete costituita, in forma unitaria o separata, da testo, suono, grafica, immagini fisse o in movimento, programmi per elaboratore e qualsiasi altro specifico di comunicazione.
- Comportamento: atto o insieme di atti posti in essere attraverso la Rete o riguardanti l'utilizzo della Rete.
- Contenuto o comportamento illecito: si tratta di contenuto o comportamento contrario alle normative vigenti in

Italia.

- Contenuto o comportamento potenzialmente offensivo: si tratta di contenuto o comportamento che pur non contrastando con le normative vigenti, e quindi lecito, può risultare offensivo per talune categorie di utenti; particolare rilevanza ha il tema della tutela dei minori.
- Soggetti di Internet: tutti i soggetti (persone fisiche o giuridiche) che utilizzano Internet.
- Utente: chiunque acceda ad Internet.
- Fornitore di infrastrutture: chiunque offra infrastrutture per Internet.
- Fornitore di accesso: chiunque offra accesso a Internet.
- Fornitore di "hosting": chiunque offra hosting su server connesso a Internet.
- Fornitore di contenuto: chiunque immetta contenuto su Internet.
- World Wide Web: insieme dei contenuti presenti su Internet e identificati da un indirizzo univoco (URL).
- Forum/gruppi di discussione/newsgroup: spazio di discussione a carattere tematico con comunicazione differita e costituito da messaggi propagati attraverso la rete su tutti i server che ospitano tale spazio di discussione.
- Chat/IRC (Internet Relay Chat): spazio di discussione con comunicazione in tempo reale.
- Posta elettronica (e-mail): sistema telematico che consente l'invio di documenti a carattere privato ad uno o più destinatari determinati dal mittente.
- Commercio elettronico: attività di compravendita di beni e servizi svolta completamente o in parte attraverso la Rete.
- Crittografia: metodo di codifica dei dati che ne impedisce la fruizione ai soggetti non autorizzati (che non posseggono la chiave per decrittare i dati); tecnica utile, ad esempio, per incrementare la privacy della corrispondenza via posta elettronica
- Comunicazione privata: una comunicazione è considerata privata quando è indirizzata esclusivamente ad uno o più destinatari determinati dal mittente.
- Comunicazione pubblica (messa a disposizione del pubblico di contenuti): una comunicazione di contenuti rivolta a destinatari non determinati individualmente dal fornitore di contenuti.
- Connessione ipertestuale o link: funzione che consente, selezionando all'interno di un contenuto una determinata parte di testo o di elemento grafico, di passare istantaneamente ad un'altro contenuto o server in qualunque punto della rete.

Le definizioni precedenti sono suscettibili di cambiamento ad opera degli organismi previsti da questo Codice sulla base dei mutamenti nello stato delle tecnologie e nella pratica ed uso della rete Internet.

2. Finalità del Codice

Il Codice di autoregolamentazione per Internet (di seguito Codice) ha l'obiettivo di prevenire l'utilizzo illecito o potenzialmente offensivo della Rete attraverso la diffusione di una corretta cultura della responsabilità da parte di tutti i soggetti attivi sulla Rete.

In particolare è obiettivo del Codice:

- fornire a tutti i soggetti della Rete regole di comportamento;
- fornire agli utenti della Rete strumenti informativi e tecnici per utilizzare più consapevolmente servizi e contenuti;
- fornire a tutti i soggetti di Internet un interlocutore cui rivolgersi per riportare eventuali casi di violazione

del presente Codice;
Il Codice definisce le regole cui devono attenersi i soggetti obbligati.

3. Campo di applicazione

3a. Soggetti obbligati

L'adesione al presente Codice è volontaria e aperta a tutti i soggetti di Internet operanti in Italia o in lingua Italiana. I soggetti obbligati all'osservanza del presente Codice sono coloro che lo abbiano sottoscritto.

3b. Clausola di estensione

I soggetti firmatari del Codice si obbligano ad estendere ai terzi l'obbligatorietà del Codice stesso attraverso la previsione di un'apposita clausola in tutti i contratti di fornitura di accesso a Internet e di hosting che verranno stipulati.

4. Principi generali del Codice di Autoregolamentazione di Internet:

4a. Principi generali di identificazione e di diritto all'anonimato.

- Tutti i soggetti di Internet devono essere identificabili.
- Qualsiasi soggetto di Internet, una volta identificato, ha diritto a mantenere l'anonimato nell'utilizzo della Rete al fine della tutela della propria sfera privata.

4b. Principi generali di responsabilità:

- Il fornitore di contenuti è responsabile delle informazioni che mette a disposizione del pubblico.
- Ogni soggetto di Internet può esercitare, contemporaneamente o separatamente, più funzioni distinte e coprire diversi ruoli.

Al fine di definire i diritti e le responsabilità individuali in rete, occorre distinguere i soggetti di Internet sulla base delle funzioni e dei ruoli esercitati in ciascun momento (e dunque indipendentemente dal fatto che il ruolo sia ricoperto in forma continuativa o occasionale, professionale o privata, a fine commerciale o meno).

- Nessun altro soggetto di Internet può essere ritenuto responsabile, salvo che sia dimostrata la sua partecipazione attiva.

Per partecipazione attiva si intende qualsiasi partecipazione diretta all'elaborazione di un contenuto.

- La fornitura di prestazioni tecniche senza conoscenza del contenuto non può presumere la responsabilità dell'attore che ha fornito tali prestazioni.

4c. Principi di tutela della dignità umana, dei minori e dell'ordine pubblico:

- Il rispetto della dignità umana comporta la tutela della vita umana e il rifiuto di ogni forma di discriminazione riferita all'origine, appartenenza, effettiva o presunta, etnica, sociale, religiosa, sessuale, allo stato di salute o ad una forma di handicap o a causa delle idee professate.
- La protezione dei minori impone il rifiuto di tutte le forme di sfruttamento, in particolare quelle di carattere sessuale, e di tutte le comunicazioni ed informazioni che possono sfruttare la loro credulità; il rispetto della sensibilità dei minori impone inoltre cautela particolare nella diffusione al pubblico di contenuti potenzialmente nocivi.
- L'utilizzo della Rete Internet impone il rispetto dei principi che regolano l'ordine pubblico e la sicurezza sociale. La Rete non deve essere veicolo di messaggi che incoraggino il compimento di reati e, in particolare, l'incitamento all'uso della violenza e di ogni forma di partecipazione o collaborazione ad attività delinquenti.

4d. Libertà fondamentali e protezione della vita privata:

- L'utilizzo corretto di Internet richiede il rispetto dei diritti e le libertà fondamentali e, in particolare, della libertà individuale, del diritto di accedere all'informazione, della libertà di riunirsi, della tutela della vita privata, della tutela dei dati personali, del segreto epistolare.

4e. Principi di tutela dei diritti di proprietà intellettuale e industriale:

- Tutte le creazioni intellettuali originali, i segni distintivi e le invenzioni sono tutelate rispetto all'autore e ai suoi aventi diritto, in conformità alle leggi italiane, alla normativa comunitaria e ai trattati internazionali che regolano la proprietà intellettuale ed industriale.

4f. Principi di tutela dei consumatori nel quadro del commercio elettronico:

- Le attività con finalità commerciale e/o professionale su Internet si svolgono in base ai principi di correttezza e trasparenza e sono soggette alla normativa italiana e comunitaria in materia di tutela dei consumatori, di vendita a distanza e in materia di pubblicità.

4g. Principi per l'applicazione del Codice di Autoregolamentazione di Internet:

- I soggetti di Internet si impegnano a promuovere l'uso del Codice e a collaborare tra di loro per trovare i modi migliori per la sua applicazione.
- Si impegnano, inoltre, ad accettare e a proporre testi contrattuali che facciano riferimento al Codice di Internet.
- I soggetti firmatari del Codice si impegnano a dare diffusione alle decisioni dell'organo giudicante e a far rispettare

le decisioni dello stesso organo adottando, eventualmente, gli opportuni provvedimenti.

· I soggetti di Internet si impegnano, nel mettere contenuti a disposizione del pubblico, a fare figurare in modo chiaro un'indicazione relativa alla loro adesione alle disposizioni del Codice.

Questa indicazione può prendere, quando ciò è ragionevolmente fattibile, la forma di un'icona (secondo il modello allegato).

Questa indicazione comporterà un link verso il testo del Codice, nonché dei link a siti direttamente o indirettamente coinvolti nel processo di autoregolazione (servizi di allarme e di reclamo).

Titolo II - Regole generali di comportamento

5. Obblighi relativi all'identificazione dell'utente

· I soggetti devono consentire l'acquisizione dei propri dati personali a chi fornisca loro accesso e/o hosting. I fornitori di detti servizi sono tenuti a registrare i dati per renderli disponibili all'autorità giudiziaria nei termini previsti dalla legge.

· Una volta identificato, l'utente può chiedere al suo fornitore di accesso e hosting di avere un identificativo diverso dal suo nome (pseudonimo) con cui operare in Rete (anonimato protetto).

6. Obblighi relativi alla tutela della dignità umana, dei minori e dell'ordine pubblico

· Qualunque soggetto di Internet venga direttamente a conoscenza dell'esistenza di contenuti accessibili al pubblico di carattere illecito, provvede ad informare direttamente l'autorità giudiziaria.

· Qualunque soggetto di Internet venga direttamente a conoscenza dell'esistenza di contenuti accessibili al pubblico in contrasto con le disposizioni del presente Codice, provvede ad informare l'organo di autodisciplina.

· I fornitori di accesso e di hosting sono tenuti a rendere facilmente accessibili in linea con ogni mezzo idoneo, compresa la posta elettronica, le informazioni circa le modalità di segnalazione alle autorità competenti dei contenuti illegali o potenzialmente dannosi dei quali vengano a conoscenza.

· I fornitori di contenuto utilizzano strumenti atti ad informare, attraverso la visualizzazione di appositi segnali, gli utenti finali della presenza di argomenti potenzialmente offensivi, in modo da impedire la visione involontaria di questi contenuti.

· I fornitori di contenuto si obbligano:

1. a rendere facilmente accessibili in linea con ogni mezzo idoneo, compresa la posta elettronica, le informazioni circa le caratteristiche tecniche, le modalità di funzionamento e gli strumenti per l'utilizzazione dei programmi di filtraggio.

2. ad eseguire una autoclassificazione dei propri contenuti in base al sistema di classificazione riconosciuto come standard dal Codice e ad accettare le variazioni alle proprie classificazioni eventualmente richieste da parte dell'organismo di autodisciplina.

La selezione del sistema standard di classificazione dei contenuti è affidata al Comitato Attuativo del Codice, tenendo in considerazione lo stato dell'arte tecnologico, la diffusione dei sistemi in ambito internazionale e, in particolar modo, la coerenza con le scelte effettuate in materia dagli altri Paesi Membri dell'Unione Europea.

7. Obblighi relativi a tutela delle libertà fondamentali e della vita privata

· Il fornitore d'accesso provvederà ad informare i propri clienti sui limiti tecnici nella protezione della segretezza della corrispondenza e dei dati nominativi e personali, esistenti in Rete.

· Il fornitore d'accesso provvederà a fornire ai suoi clienti indicazioni sulle misure e sui prodotti - che non violino le vigenti normative - destinati ad assicurare la riservatezza e l'integrità della loro corrispondenza e dei loro dati, in particolare per ciò che riguarda gli strumenti di crittografia e/o firma elettronica.

7a. Segretezza della corrispondenza:

· Lo scambio della corrispondenza privata in Internet è fondata sulle disposizioni di legge che regolano il segreto epistolare.

Al dovere generale di riservatezza e di vigilanza sulla riservatezza sono tenuti, con particolare rigore, i soggetti che svolgono attività commerciali e/o professionali in Rete.

· Le aziende che impiegano personale con facoltà di accesso - per motivi professionali - alla corrispondenza privata si obbligano al rispetto della segretezza e a richiamare l'attenzione dei loro collaboratori circa la responsabilità penale che potrebbe derivare dalla violazione di tale segretezza.

7b. Dati nominativi e personali:

- Le informazioni di carattere nominativo e personale trasmesse volontariamente dall'abbonato o involontariamente durante la connessione tra elaboratori in Rete devono essere raccolte ed utilizzate nel rispetto dei diritti del soggetto a cui si riferiscono e, soprattutto, nel rispetto della normativa vigente in materia di trattamento dei dati personali.
- I fornitori di accesso attraverso collegamenti temporanei della rete telefonica pubblica sono tenuti a conservare la data, gli orari e il numero di IP assegnato delle connessioni effettuate da ciascuno dei propri utilizzatori per un termine di 24 mesi dalla connessione. I fornitori di accesso attraverso collegamenti dedicati sono tenuti a mantenere un registro degli indirizzi di rete assegnati ai propri clienti.

8. Obblighi relativi alla tutela dei diritti di proprietà intellettuale e industriale

- Tutte le creazioni intellettuali originali sono tutelate rispetto all'autore e ai suoi aventi diritto, in conformità alla legge italiana sul diritto d'autore, alla normativa comunitaria e ai trattati internazionali.
- Le basi di dati sono soggette a tutela a favore dei loro autori ed aventi diritto, in base alla legge sul diritto d'autore e alle norme specifiche che regolano i diritti sulle basi di dati.
- Un'opera non può essere riprodotta o essere messa a disposizione del pubblico senza l'autorizzazione del titolare dei diritti.
- Le indicazioni relative all'autore dell'opera, al titolare dei diritti e all'identificazione numerica dell'opera non possono essere eliminate o modificate senza il consenso delle persone interessate.
- La trasmissione automatizzata delle opere per l'inserimento sulla rete non è considerata una forma di riproduzione dell'opera.
- La citazione dell'opera attraverso collegamenti ipertestuali con altri siti è lecita.

Ogni forma di citazione implicante la riproduzione dell'opera deve essere effettuata nel rispetto delle norme specifiche. La citazione dell'opera soggetta a tutela, in particolare, deve:

- indicare il nome dell'autore, la fonte e non deve alterare gli elementi che permettono l'identificazione numerica;
 - essere breve;
 - essere incorporata in un'altra opera;
 - essere giustificata dalla natura dell'opera in cui essa è incorporata.
- Le norme che regolano il marchio sono applicabili ai soggetti di Internet.
 - I soggetti di Internet si astengono dalla riproduzione sostanziale dei contenuti di un sito altrui senza autorizzazione, anche se questi non sono soggetti alla tutela del diritto d'autore. In particolare, i fornitori di contenuto, prima di qualunque utilizzo di opere soggette a tutela, devono assicurarsi di avere ottenuto i relativi diritti ed autorizzazioni dagli aventi diritto.
 - I fornitori di hosting devono prevedere nei contratti con i clienti una clausola che richiama tale principio.
 - Nel momento in cui termina il mantenimento del contenuto su un sito o su un server, per conclusione del rapporto contrattuale o per altra causa, il fornitore del servizio, in conformità alle disposizioni contrattuali, cessa di conservare i dati forniti dal suo cliente.
 - Prima di compiere qualunque utilizzazione su Internet di un segno destinato a distinguere un prodotto o un servizio o ad indicare l'indirizzo di un sito, il fornitore di contenuto che intende utilizzare tale segno deve verificare la disponibilità di esso.

9. Obblighi generali relativi ad attività commerciali e/o professionali particolari:

9a. Consulenze

I servizi che offrono informazioni o consulenze citando opinioni devono indicare chiaramente l'identità, la qualifica professionale, l'eventuale carica ricoperta dall'esperto o specialista.

Tale indicazione deve comunque essere fornita nel rispetto delle norme deontologiche che vietano, per alcune categorie di professionisti, qualsiasi forme di pubblicità.

Ogni servizio deve essere fornito in termini e con modalità che riflettano la serietà della disciplina oggetto della consulenza, soprattutto nel caso di servizi di consulenza medica.

9b. Servizi informativi

I servizi che offrono informazioni su dati, fatti o circostanze suscettibili di subire variazioni nel corso del tempo devono contenere anche l'indicazione della data e dell'ora a cui risale l'aggiornamento della informazione fornita.

9c. Manifestazioni a premio

Qualsiasi servizio che istituisca una manifestazione a premio potrà essere attivato solo dopo che sia stato emesso il relativo decreto di autorizzazione da parte del Ministero delle Finanze o, nel caso di operazioni a premio limitate ad una sola provincia, della competente Intendenza di Finanza, ai sensi della disciplina dettata dal R.D.L: 29.10.1938 n. 1933 e succ. mod., convertito in legge 27.11.1989 n.384, e dal R.D. 25.7.1940 n.1077.

9d. Opportunità di lavoro

Un fornitore di contenuto, prima di attivare un servizio di promozione delle opportunità di lavoro, deve assicurarsi che la fornitura del servizio non implichi una violazione della disciplina sull'intermediazione e/o sull'interposizione dei lavoratori.

I servizi che offrono corsi d'addestramento professionale o altri corsi d'istruzione hanno l'obbligo di non formulare irragionevoli promesse o previsioni di futuro impiego o di futura remunerazione nei confronti degli utenti.

9e. Pubblicità

Il fornitore di contenuti si impegna a rispettare la normativa di cui al Codice di Autodisciplina Pubblicitaria, sia per la pubblicità a favore dei servizi offerti, veicolata attraverso gli stessi servizi o attraverso altri mezzi, sia per la pubblicità volta a promuovere altri servizi o prodotti, in cui il servizio rappresenta unicamente il veicolo di diffusione.

Il fornitore di contenuti si impegna a offrire a particolari condizioni spazi pubblicitari per la comunicazione di rilevanza sociale, in base alle stesse norme previste per la pubblicità radio televisiva.

Titolo III - Applicazione del Codice

10. Premessa

Gli operatori che hanno sentito l'esigenza di darsi regole di comportamento nell'utilizzo di Internet, facendosi promotori del presente Codice, nelle persone dell'Associazione Italiana Internet Providers, dell'Associazione Nazionale Editoria Elettronica, di Olivetti e di Telecom Italia ritengono opportuno riunirsi volontariamente in un Comitato Attuativo che si prefigge, tra gli altri sottoindicati, l'obiettivo di nominare i membri di un Giurì preposto alla tutela del presente Codice. Il Comitato Attuativo potrà anche rendersi promotore della creazione di una struttura associativa stabile finalizzata alla diffusione ed al sostegno del presente Codice, dotata di statuto e di appositi organi amministrativi. In tale evenienza, le disposizioni che seguono avranno carattere transitorio.

11. Comitato Attuativo

Costituzione e composizione

I promotori del presente Codice costituiscono volontariamente, ai sensi degli artt. 36 e seguenti del Codice Civile, un Comitato Attuativo del Codice medesimo ed eleggono domicilio presso :

Il Comitato Attuativo è composto da tre rappresentanti per ogni promotore.

Nella prima seduta il Comitato Attuativo elegge tra i suoi membri un Presidente ed un Vice Presidente e costituisce un fondo comune, ai sensi dell'art.37 del Codice Civile, destinato al finanziamento delle attività a cui il Comitato ed il Giurì sono preposti.

Funzioni e compiti

Le funzioni del Comitato Attuativo sono l'informazione, la prevenzione e la regolamentazione.

I compiti affidati al Comitato Attuativo sono:

- l'attuazione e l'evoluzione del presente codice attraverso raccomandazioni ed emendamenti;
- la nomina dei membri del Giurì di Autotutela;
- l'esame, in seconda istanza, dei ricorsi su decisioni prese dal Giurì;
- un ruolo di informazione e di consultazione per gli utenti ed i soggetti di Internet;
- la conciliazione (attraverso forme di mediazione ed arbitrato) tra i soggetti di Internet;
- la realizzazione e gestione di un sito Internet con funzione di diffusione dei principi del Codice, di informazione per tutti i soggetti di Internet sull'autoregolamentazione, di supporto per l'attività del Giurì;
- lo sviluppo dei rapporti con le autorità pubbliche, le autorità indipendenti e le associazioni di categoria a livello nazionale e internazionale;
- lo sviluppo dei rapporti con organismi corrispondenti di altri paesi;
- attività di studio e di ricerca.

Riunioni

Il Presidente, d'intesa con il Vice Presidente, convoca le riunioni del Comitato Attuativo, stabilendo l'ordine del giorno dei lavori. Il Comitato si riunisce in via ordinaria almeno 2 volte all'anno e in via straordinaria quando richiesto dal Presidente o da almeno un terzo dei componenti. In tale caso la riunione deve svolgersi entro 15 giorni dalla presentazione della richiesta.

12. Giurì di Autotutela

Costituzione e composizione

Il Giurì di Autotutela è costituito ad opera del Comitato Attuativo, è composto da cinque membri designati e nominati dal Comitato Attuativo ed è domiciliato presso:.....

Durata

I membri del Giurì di Autotutela restano in carica un anno, con possibilità di riconferma per i suoi membri da parte del Comitato Attuativo.

Presidente e Vicepresidente

Nella prima seduta il Giurì di Autotutela elegge tra i suoi membri un Presidente ed un Vice Presidente.

Funzioni

Le funzioni del Giurì di Autotutela sono: la tutela del rispetto del presente Codice, l'intervento in caso di segnalazione di infrazioni da parte di soggetti Internet, di consumatori o di chiunque vi abbia interesse, l'accertamento e la pronuncia su eventuali infrazioni e l'applicazione di sanzioni nei confronti dei soggetti ritenuti responsabili.

Inoltre il Giurì può inoltre esprimere pareri preventivi sulla conformità al Codice di informazioni da mettere a disposizione del pubblico, sulla congruità ai principi del rating di particolari contenuti e sui criteri di autocertificazione.

13. Procedure

Segnalazione e istruttoria

La segnalazione di infrazioni deve essere effettuata da parte dei soggetti di Internet attraverso una istanza, da inviarsi via posta elettronica (oppure via servizio postale o via fax), contenente la descrizione dell'infrazione, l'indicazione dell'URL del sito relativo all'infrazione denunciata.

Ricevuta la denuncia, il Presidente del Giurì apre un procedimento istruttorio, fissa un termine per la decisione e sceglie all'interno del Giurì un membro istruttore incaricato di:
(a) notificare alle parti interessate l'apertura del procedimento istruttorio, la convocazione per la discussione, concedendo loro un termine di 3 giorni per il deposito di eventuali deduzioni e/o documenti;
(b) esaminare l'istanza segnalata e di preparare una relazione sulla fattispecie denunciata, con potere di interpellare le parti interessate.

Allo scadere di tale termine, il Presidente convoca il Giurì, che ha l'obbligo di assumere una decisione in merito al procedimento, sulla base della relazione dell'istruttore e delle deduzioni e/o documenti depositati dalle parti interessate.

Al Giurì è data, peraltro, facoltà di prorogare il termine per la decisione qualora il procedimento non risulti sufficientemente istruito o sia necessario acquisire ulteriori elementi ai fini della decisione, dandone comunicazione alle parti.

Decisione e sanzioni.

La decisione del Giurì viene immediatamente notificata alle parti e deve contenere il provvedimento che sarà conseguentemente adottato, con relativa motivazione.

In caso di pronunciamento negativo, ovvero se la decisione stabilisce l'insussistenza dell'infrazione segnalata, il Giurì provvede a chiudere il procedimento.

In caso di pronunciamento positivo, ovvero se la decisione stabilisce che sussiste l'infrazione segnalata, il Giurì adotterà i seguenti provvedimenti:

1. comunicazione di diffida, contenente l'invito a conformarsi al pronunciamento del Giurì entro il termine di 2 giorni.
2. in caso di inosservanza del provvedimento di cui al punto 1, formale ammonimento da pubblicarsi sul sito relativo all'organismo di autoregolamentazione Internet, con sollecito ad adempiere alla diffida di cui al punto 1;

Le decisioni ed i conseguenti provvedimenti sono vincolanti nei confronti di tutti i soggetti aderenti al presente Codice.

Le parti possono presentare opposizione entro il termine di 3 giorni al Comitato Attuativo, il quale,

- (a) ove ritenga fondate le ragioni dell'opponente, ha facoltà di modificare o annullare, con atto motivato, la decisione del Giurì;
- (b) in caso contrario, il Comitato Attuativo conferma, con atto motivato, la decisione presa dal Giurì.

14. Contenuti e azioni illecite

Nel caso di segnalazione di contenuti o comportamenti che risultino, oltre che in violazione del presente Codice, pure

illeciti, il Giurì si rivolge direttamente all'Autorità giudiziaria garantendo la massima collaborazione per il proseguo delle indagini.

I fornitori di servizi informano i loro clienti della loro facoltà di sospendere e bloccare la diffusione dei contenuti illeciti in applicazione degli avvisi dell'Autorità giudiziaria .

VI. UK -ISPA Code of Practice

Adopted 25 January 1999

Preamble

- (a) This Code of Practice (*Code*) shall govern the conduct of the Members (as defined below) of the UK Internet Services Providers Association (*ISPA*). The application of the Code shall be uniform and obligatory to all Members without modification or exception. A Member may not, by contract or otherwise, evade the application of the Code.
- (b) The Council (as defined below), or such of its officers as it may nominate, shall administer the Code. The administration of the Code shall be reactive only - the Council will not monitor Members' activities for breaches of the Code.
- (c) From time to time the Council may issue policy statements regarding matters relating to the regulation of the Internet in the UK. After due and proper consultation with the Members, such policy statements may be adopted as practice statements by ISPA (*ISPA Practice Statements*). Such Practice Statements shall be incorporated into the Code and shall thereby be binding on Members. The Code may be further amended from time to time in accordance with the Articles.
- (d) Members agree that, as an ISPA member, they must abide by the Code and support agreed ISPA Practice Statements.
- (e) For the avoidance of doubt, and save for any express provisions to the contrary, nothing in the Code shall be taken to suggest that the Code regulates and/or that the Council will adjudicate on the legality or otherwise of material accessible on the Internet, whether by Members or otherwise. Where a Complaint (as defined below) concerns the legality of such material, the Secretariat (as defined below) will advise the Complainant to contact the originator of the material directly.
- (f) Members recognise that compliance with the Code does not necessarily guarantee that they are acting within the law. Any reference in the Code to lawfulness or unlawfulness relates solely to UK law.

CODE OF PRACTICE

1. Interpretation

1.1 Unless otherwise stated, capitalised terms in this document shall have the following meanings:

<i>Articles:</i>	Articles of Association of ISPA.
<i>Chief Executive:</i>	Chief Executive of ISPA.
<i>Council:</i>	ISPA Council.
<i>Customer:</i>	Customer of a Member.
<i>Complaints Procedure:</i>	The complaints procedure set out in Clause 8.4 below.
<i>Hacking:</i>	Denial of service attacks and other forms of hacking.
<i>Members:</i>	Full members of ISPA, ie those members which have the right to receive notice of, attend and vote at any general meeting of ISPA, and to nominate candidates in any election for the Council.
<i>IWF:</i>	Internet Watch Foundation.
<i>Promotional Material:</i>	Material promoting any Services.
<i>Secretariat:</i>	ISPA Secretariat.
<i>Services:</i>	Services provided by any Member.
<i>Spam:</i>	Unsolicited advertising material or information sent to an e-mail address or newsgroup.
<i>Spamming Software:</i>	Computer software used for filtering out Spam prior to it reaching e-mail addresses and/or newsgroups.
<i>Terms and Conditions:</i>	Any Member's standard terms and conditions governing the provision of Services to its Customers.
<i>Third Party Content:</i>	Material accessible via a Member's Service, which originates from and/or is owned by one or more third parties (including, for the avoidance of doubt, that Member's Customers).

- 1.2 In this document, any reference to an enactment or statutory provision is a reference to it as it may be amended or re-enacted, and any reference to a code of practice is a reference to it as it may be amended or re-issued.

2. General Requirements

2.1 Legality

Members shall use their reasonable endeavours to ensure the following:

- 2.1.1 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.
- 2.1.2 Members, their Services (excluding Third Party Content) and Promotional Material do not encourage anything which is in any way unlawful.

2.2 Decency

Members shall use their reasonable endeavours to ensure the following:

- 2.2.1 Services (excluding Third Party Content) and Promotional Material do not contain material inciting violence, cruelty or racial hatred.
- 2.2.2 Services (excluding Third Party Content) and Promotional Material are not used to promote or facilitate practices which are contrary to UK law.

2.3 Honesty

- 2.3.1 Members shall use their reasonable endeavours to ensure Services (excluding Third Party Content) and Promotional Material are not of a kind that are likely to mislead by inaccuracy, ambiguity, exaggeration, omission or otherwise.

2.4 Fair Trading

- 2.4.1 In its dealings with consumers, other businesses and each other, Members must act decently, fairly and reasonably at all times.
- 2.4.2 Members must, upon request, bring to the attention of their Customers the existence of the Code and must notify any Customer of the Complaints Procedure, where that procedure is available to the Customer.

2.5 Customer Contracts

- 2.5.1 Members shall ensure that they bring their Terms and Conditions to the attention of all new Customers before such Customers register with a Member for Services.
- 2.5.2 Members must include in their contracts with Customers a provision requiring Customers to comply with the UK law in using any of the relevant Member's Services.

3. Promotion

3.1 Scope

- 3.1.1 Members must use all reasonable endeavours to ensure that Promotional Material transmitted by radio, television, teletext, telephone, facsimile or any other form of communication must observe the provisions of this Code and the Codes of Practice published by the Independent Television Commission and the Radio Authority (where relevant) in the manner most reasonable and appropriate to the technology employed.
- 3.1.2 Promotional Material must also comply with the provisions of the British Codes of Advertising and Sales

Promotion which are supervised by the Advertising Standards Authority.

3.1.3 Services and Promotional Material shall comply with the Code of Practice applied by ICSTIS when access to them is made via a premium rate telephone call.

3.1.4 In addition to the codes of practice referred to in Clauses 3.1.1 to 3.1.3 above, Members must also comply with any other code of practice expressly regulating Promotional Material.

3.2 *Pricing Information*

3.2.1 Members must ensure that charges for Services are clearly stated in relevant Promotional Material. Members must make clear whether any such charges quoted are inclusive or exclusive of VAT. Where additional charges, for example on-line charges, are payable this should be stated.

3.2.2 Members must use reasonable endeavours to ensure that textual pricing information relating to charges for Services is accurate, up to date, legible, prominent and presented in such a way that does not require close examination.

4. Data Protection and Privacy

4.1 Members shall comply with UK legislation relating to data protection.

4.2 When registering with the Data Protection Registry, all Members must in their application state that the data may be used for regulatory purposes and that ISPA is a potential user of that information.

4.3 Where Services involve the collection of personal information, such as names and addresses, from individuals (*Data Subjects*), Members must make it clear to Data Subjects the purpose for which such information will be used. Members must also identify the data user (if different from the Member or Data Subject) and give the Data Subject the opportunity to object to such usage.

5. IWF

5.1 ISPA co-operates with the IWF in its efforts to remove illegal material from Internet web-sites and newsgroups. Members are therefore required to adhere to the IWF procedure, as follows.

5.1.1 Members must register with the IWF to receive notices and provide the IWF with a point of contact.

5.1.2 Members may from time to time receive notices from the IWF requesting prompt removal of specified material from web-sites or newsgroups which those Members are hosting; provided they are technically able to do so, Members must comply with such notices within a reasonable time and simultaneously inform the originator of such material if such originator is their Customer.

5.1.3 Where requested by the IWF (on behalf of a legitimate law enforcement authority), and where technically able to do so, Members must retain copies of removed material for a reasonable period of time.

6. Transfer of Domain Names

6.1 Members must offer Customers the option of retaining their respective domain name(s), other than where such domain name(s) are sub-domains of the relevant Member's own name, where Customers choose to transfer to another ISP (whether that ISP is a Member or not). Where a Customer elects to retain such name(s), the relevant Member must transfer such name(s) within five working days of the Customer transferring to another ISP, or as soon as the Customer has paid all sums owed to the relevant Member in respect of the original registration of such name(s).

6.2 The time limits in clause 6.1 shall not apply where the relevant Member's Terms and Conditions require that sums relating to all Services be paid prior to transfer of any domain name(s) and that the Member continues

to act as the Customer's agent in respect of any domain names until such payment.

7. Best Practice

- 7.1 ISPA recommends that Members adhere to the following best practice guidelines where possible:
 - 7.1.1 Members should provide guidance to Customers about the availability of tools which may assist them in filtering content which Customers deem unsuitable ("Filtering Software").
 - 7.1.2 Members should follow best industry practice in offering Customers Filtering Software.
 - 7.1.3 Members should provide to the Police a 24-hour point of contact.
 - 7.1.4 Members should endeavour, where possible, to respect any caching directions or restrictions of which they are advised by Customers whose web-sites they host.
 - 7.1.5 Members should advise Customers regarding any software tools which they can use to protect their privacy.
 - 7.1.6 Members should follow the best industry practice in using Spamming Software, such that Customers can elect to minimise the amount of Spam sent to their e-mail account.
 - 7.1.7 Members should include on their web-sites the ISPA logo, with a link to the ISPA web-site.