Self-regulation of Internet Content

Self-regulation of Internet Content

Bertelsmann Foundation
Gütersloh 1999

Responsible: Dr. Marcel Machill, Jens Waltermann
Cover design: Tammen Werbeagentur, Osnabrück
Cover photos: Tony Stone/Tammen Werbeagentur, Osnabrück
Typesetting: digitron GmbH, Bielefeld
Print: ReproZentrum Rosenberger GmbH & Co., Bielefeld

Contents

Key Recommendations

1. The Internet: changing the way people live

As an international community of users and providers of information, we are at a dramatic turning point. The Internet will change the way people live: it offers extraordinary opportunities for enhancing creativity and learning, for trading and relating across borders, for safeguarding human rights, for realizing democratic values and for strengthening pluralism and cultural diversity. The change holds promise and it holds challenges. Although a limited phenomenon within the overall amount of Internet content, racist and discriminatory web sites, child pornography exchanged in certain newsgroups and chatrooms and "how to" guides for terrorist activities are too disturbing to ignore. Mechanisms have to be developed to deal with illegal

content, to protect children online as well as guarantee free speech.

2. Self-regulation of Internet content: towards a systematic, integrated and international approach

No single approach, relying on one form or one set of actors, can provide a solution to content concerns in the changing and shifting environment that is the Internet. For a public response to be effective, it must be integrated, systematic and dynamic, sensitive to public needs and national differences within a framework that encourages robust communication. Only such a systematic approach – bringing technological potential together with the energies and capacities of government, the Internet industry and the citizenry – has the promise of success in meeting what often seem to be competing goals. Given the global and borderless architecture of the Internet, such a systematic approach requires not only coordination at a national and regional level, but its scope must be international.

3. Internet industry: developing and implementing codes of conduct

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 operate as an accountability system that guarantees a high level of credibility and quality. As part of

the codes of conduct, Internet providers hosting content have an obligation to remove illegal content when put on notice that such content exists. The procedure for such notice and take-down – while laid down by regulation – should be reflected in codes of conduct and should specify the requirements for proper notification of service providers. The service provider may include in its contracts with users and content providers terms which allow it to comply with its legal obligations and protect it from liability. It is in the best interest of industry to take on such responsibility since it enhances consumer confidence and is ultimately good for business.

4. Sharing responsibility: self-regulatory agencies enforcing codes of conduct

To be effective, codes of conduct must be the product of and be enforced by self-regulatory agencies. Such agencies must be broadly representative and accessible to all relevant parties. Subject to a process of acquiescence by public authorities they should enjoy certain legal privileges enhancing their functions. Effective self-regulation requires active consumer and citizen consultation by such agencies. 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.

5. Governments: supporting and reinforcing self-regulation

Self-regulation cannot function without the support of public authorities, be it that they simply do not interfere with the self-regulatory process, be it that they endorse or ratify self-regulatory codes and give support through enforcement. There are clearly limits to what can be achieved by self-regulation. The process cannot alone guarantee that child pornographers are caught and punished, although self-regulatory mechanisms can help ensure that criminals cannot use the Internet with impunity. Governments should, through education and public information, raise awareness among users about self-regulatory mechanisms such as the means to filter and block content and to communicate complaints about Internet content through hotlines.

6. Self-rating and filtering systems: empowering user choice

Filtering technology can empower users by allowing them to select the kinds of content they and their children are exposed to. Used wisely, this technology can help shift control of and responsibility for harmful content from governments, regulatory agencies, and supervisory bodies to individuals. Thus, at the core of the recommendations for an integrated system of self-regulation and end user autonomy must be an improved architecture for the rating and filtering of Internet content. There should be an independent organization to provide a basic vocabulary for rating and to oversee updates to the system at periodic intervals.

Content providers worldwide must be mobilized to label their content and filters must be made available to guardians and all users of the Internet.

7. Internet filtering: ensuring youth protection and freedom of speech

A good filtering system realizes several important values: end user autonomy; respect for freedom of expression; ideological diversity; transparency; respect for privacy; interoperability and compatibility. Equally important, the system must feature a user-friendly interface that encourages actual use of its features and makes choice a real possibility for the vast majority of end users. Third parties should be encouraged to develop and provide free filters. Industry should promote the availability and use of filtering systems, educating consumers about how to filter and making it easy for parents, teachers, and other concerned adults to choose filters, install and adapt them to their set of values. Regulatory requirements on service providers to screen or filter content should be avoided. Government or regulatory agencies may supply filters but should *not* mandate their use.

8. Hotlines: communicating and evaluating content concerns

We need technical and organizational *communication* devices to ensure that users can respond to content on the Internet that they find of substantial concern. These "hotlines" ensure that – where necessary and appropriate –

effective action can be taken to remedy such concerns. The task of evaluating the legality or illegality of specific data is difficult for Internet providers and should, therefore, be integrated into the work of hotlines. In order to function, hotlines need an environment and operational rules that honor their specific task of handling problematic – and perhaps illegal – content. Legislators should formulate minimum requirements on the organizational setup and procedures of hotlines and, in turn, shield them from criminal or civil liability incurred in the proper conduct of their business ("safe harbor").

9. International cooperation: acting against content where it is located

There should be an international network of hotlines governed by a framework agreement containing minimum standards on the handling of content concerns and stipulating mutual notification between hotlines. The hotline in the country where the content is located is asked to evaluate it and to take action. This mechanism results in content providers being acted against only if the material is illegal in the host country. The mechanism also overcomes difficulties in the complex diplomatic procedures necessary for cross-border cooperation of law enforcement authorities.

10. The legal framework: limitations on liability

There should be no criminal responsibility of mere access and network providers for third parties' illegal content

transmissions taking place in real-time through their networks. Host service providers merely storing third party content should be held liable only if they have actual knowledge of illegal content, and if a removal of such content its technically possible and can reasonably be expected. Providers party to an enforceable and broadly representative self-regulatory regime, recognized by public authorities, should not be liable for third party content when complying with the requirements of that regime and the decisions of the relevant self-regulatory body.

11. Law enforcement: cooperation and continuous training

It should be a top priority to create adequate law enforcement bodies to combat computer crime and illegal content like child pornography on the Internet. This requires the development of centralized units and/or a better coordination of existing competent bodies. Such units must have adequate technical know-how and on-going training. The Internet industry should cooperate in training. Law enforcement and the Internet industry should develop cooperative structures to exchange views on common points of concern.

12. A "learning system": education and constant evaluation

No self-regulatory mechanism can work independently of an education and awareness campaign. The Internet indus-

try should develop a continuous online and off-line effort to provide general awareness of self-regulatory mechanisms such as filtering systems and hotlines. Schools should provide the necessary skills for children to understand the benefits and limitations of online information and to exercise self-control over problematic Internet content. The Internet is, itself, a process, an enormous system for change and response, feedback and transformation. Like the Internet, the legal system and self-regulatory mechanisms around it must incorporate similar practices of learning and changing. The integrated system recommended here depends on continuous (re-)evaluation.

Bertelsmann Foundation
Gütersloh, Germany, September 1999

1 Introduction

Everywhere, citizens, governments and industry are seeking to maximize the potential of the great new information technology that is the Internet. More than any medium that has come before it, this interactive tool empowers its users with the freedom to communicate, to distribute, to seek and gather information, to develop and disseminate opinions. Extraordinary opportunities for enhancing creativity and learning, for trading and relating across borders, for safeguarding human rights, for realizing democratic values and for strengthening pluralism and cultural diversity are clearly inherent in the new world heralded by the Internet. The new information technology will improve openness, transparency and efficiency at all levels in public as well as private domains. The Internet will change the way people live. Such change holds promise and it holds challenges.

An important challenge comes from illegal and harmful content. Although a limited phenomenon within the broad range and staggering volume of all Internet content, racist and discriminatory web sites, child pornography exchanged in certain newsgroups and chatrooms and "how to" guides on terrorist activities are too disturbing to be ignored. Such illegal material is a topic of broad debate. It leads to uncertainty about the capacity of existing legal approaches to effectively curb Internet misuse.

Another challenge is posed by content harmful to children yet legal when consumed by adults. While there are legal and cultural differences between countries in what is considered harmful to children, most countries have restricted the distribution of, for example, sex-related and violent material in traditional broadcast media. Governments have, however, hesitated to apply the same rules to the Internet because of mere extension of existing rules, the different nature of the medium. They would simply not work in a medium that is available anywhere around the world at any time of day or night. The significance of harmful content will become even more politically sensitive as access to the Internet through television and telephones becomes ever broader and more pervasive.

Mechanisms have to be developed to deal with illegal content and to protect children online. But they also have to protect free speech. Even if not targeted directly, browsing, surfing, or following suggestions from search engines may lead to material containing unwanted, troublesome, offensive as well as surprising or amusing material. This mixture of the deliberately sought for and the unexpected may well be one of the attractions of the medium. To be able to profit from this opportunity, to make such encoun-

ters possible, while still allowing for the protection of children and for selective approaches to information gathering and communication, is perhaps one of the most important tasks in further developing the Internet. The power of self-regulation must be harnessed to take up this task, to increase citizen confidence and to reach the full economic, cultural and social potential of the new technologies. The private sector had an important role in the creation of these technologies and in their development and use. Partnership between the public and private sector is now needed to maximize the benefit of these technologies and to minimize their risks.

The Bertelsmann Foundation has, over the last nine months, brought together a global network of representatives from government, industry, law enforcement, non-government organizations as well as scholars and experts to make recommendations concerning these questions and to advise on the structure and implementation of an internationally coordinated approach.[1] The group examined best practices, a variety of legal approaches and was asked to focus particularly on the contribution self-regulation can make to the current keen anxiety with regard to illegal and harmful Internet content. The Foundation's aim was to expand awareness among the key stakeholders of the role self-regulation can play and to do so with the geographical, professional and disciplinary variety necessary for so expansive and complex a task.

The memorandum that follows undertakes the difficult task of summarizing the results of the rich and complex interchange within the network of expert professionals,

1 Appendix I and II

industry and non-profit representatives, officials and academics. The memorandum is addressed to governments, the Internet industry and users, to regulatory and law enforcement authorities, to self-regulatory initiatives, to childrens' advocates and user-representatives. All will have to take on responsibility for Internet content. Cooperation among all will be needed to put these recommendations into practice.

2 Toward a Systematic Approach

As an international community of users and providers of information, we are at a dramatic turning point. The architecture of speech, with all its implications for political life and democracy, is being radically altered. Societies are coping with the consequences of harmful and offensive content at a moment of rapidly changing information technologies. Entire structures for the delivery and reception of speech are being transformed. Habits, patterns, laws designed to protect against specific harms are potentially challenged by global, interactive and decentralized services.

We have not only learned how *to deal with* content concerns in the more traditional media, we also have culturally learned *to live with* varying degrees of insecurity, with communication risks; we have learnt how to decide which

risk levels to accept and which to refuse, which "back-up" mechanisms to use.

No single approach, relying on one form or one set of actors, can provide a solution in such a changing and shifting environment. For a public response to be effective, it must be integrated, systematic and dynamic, sensitive to public needs and national differences within a framework that encourages robust communication. Only such a systematic approach – bringing technological potential together with the energies and capacities of government, industry and citizenry – has the promise of success in meeting what often seem to be competing goals. Given the global and borderless architecture of the Internet, such a systematic approach requires not only coordination at a national and regional level, but its scope must be international.

A systematic, self-regulation-based approach is especially desirable because the alternative – reliance on overbroad, highly intrusive regulation, with laws differing across national borders – yields short-term, often crisis-driven, mostly ineffective solutions. And these responses cannot meld together the complicated political and social objectives in a successful way. The illusion of action is no substitute for a considered and comprehensive, flexible and dynamic approach.

Content concern response systems are necessary to manage the disturbances the Internet can hold. Processes and institutions have to be developed, tested and implemented, and learning processes have to be initiated that help to create trust and to empower users.

3 Self-regulation as a Foundation

Meaningful and effective self-regulation provides the opportunity to adapt rapidly to the quickening technical progress globally and, when properly encased in collaboration with government, is preferable to mandatory governmental regulation. The general benefits of self-regulation include efficiency, increased flexibility, increased incentives for compliance, and reduced cost. A carefully structured program emphasizing self-regulation is especially harmonious with an Internet setting because it mirrors the Internet itself, as a global, essentially private and decentralized 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 accurate-

ly reflect user needs, will not be effective in delivering the standards it promotes, and will fail to create confidence.

The development of a self-regulatory regime for the Internet must comprise several complementary actions, tools and mechanisms. Moreover, self-regulation cannot function without the support of public authorities, be it that they simply do not interfere with the self-regulatory process, be it that they endorse or ratify self-regulatory codes and give support through enforcement. There are clearly limits to what can be achieved by self-regulation. It cannot, for example, by itself ensure that child pornographers are caught and punished, although self-regulatory mechanisms can be of assistance in ensuring that criminals cannot use the Internet with impunity.

The creation of self-regulatory mechanisms should, to the extent possible, be the product of cooperation or collaboration between state bodies and the Internet Service Provider (ISPs) or self-regulatory bodies. Self and legal regulation should each complement the other in relevant areas. Developing an ideal synthesis involves interweaving their specific instruments, not merely adding both together – a process best achieved through dialogue among all the parties concerned.

Another major challenge in self-regulation is the prevention of a "free-rider phenomenon" where some actors expend significant resources on the development, monitoring and implementation of codes and standards, while others simply profit from their existence or ignore them altogether. The effectiveness of self-regulation will depend largely on the full collaboration and commitment among all industry players such as content providers, service providers, and relevant software and technology industry.

It is in the best interest of industry to develop self-regulatory mechanisms as they enhance consumer confidence and are ultimately supportive of business objectives. More people will migrate online when they are confident that their families will not be exposed to harmful content. With regard to the implementation of an effective self-regulatory system, the following points are of crucial importance.

First, codes of conduct should be adopted to ensure that Internet content and service providers act in accord with the law and 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.

Second, to be effective, these codes of conduct must be the product of and be enforced by self-regulatory agencies.

Third, because of the transnational nature of Internet communications, coordinated activity among such agencies in different jurisdictions is an essential element of self-regulation.

Fourth, effective self-regulation is not possible without the support of law making and regulation including legislation that embraces and empowers the self-regulatory process.

Fifth, there should be comprehensive use of rating and filtering technology. To this end content, providers worldwide must be mobilized to label their content, and filters must be made available to empower guardians and all users of the Internet to make more effective choices about the content they wish to have enter their homes.

Sixth, a comprehensive self-regulatory system also requires content response and complaints systems for users, such as hotlines.

Seventh, awareness among users of the means to filter and block content, to redress complaints and of the level of conduct that is promised by the industry is crucial to the success of any self-regulatory framework. Education by public and information distribution by private entities must work hand in hand to raise this awareness.

Finally, techniques must be found to measure the effectiveness of self-regulatory mechanisms and to determine what national and transnational measures – if any – are necessary to compensate for their deficiencies.

With respect to these recommendations and the discussion of codes of conduct that follows, it is important to recognize and allow for national/cultural differences. The implementation and practical expression of these recommendations is likely to vary from country to country and this needs to be respected in order to avoid perceptions of the Internet as furthering monocultural imperialism.

As to Codes of Conduct, they should be endorsed as a front-line mechanism for addressing content issues and be based upon industry's social responsibility. In particular, they should distinguish between illegal content and the protection of minors from potentially harmful content. They should delineate the mechanisms through which self-regulation will occur, including provisions for cooperation with end users as well as public authorities.

Industry-wide codes may be more useful instruments of protection than those developed by small groupings of companies within sectors. They are more comprehensive and transparent which prevents confusion among users.

Internet Service Providers provide a technical service (access to the Internet, hosting content or both). They are not in the business of telling their customers what they

should or should not access, nor should they be expected to exercise control over what content is published. On the other hand, they have an obligation to take steps to remove illegal content when put on notice that such content exists. The procedure for such notice and take-down while laid down by law should be reflected in codes of conduct and provide for the interests of all involved to be respected. An ISP may include in its contracts with users and content providers terms which allow it to comply with its legal obligations and protect it from liability. In this process of cooperation, self-regulation must not become an engine for greater control than would occur if the state, itself, established all standards.

Recommendations for governments

- Government bodies should encourage and incentivize self-regulatory initiatives by industry as an efficient, flexible and cost-effective mechanism to address Internet content concerns that can secure a high degree of compliance.
- Governments should consider a process of acquiescence or ratification of codes of conduct developed by industry and may want to consider supporting their enforcement.
- In carefully specified instances, government should protect the capacity of self-regulatory agencies to handle and disclose information on illegal content to law enforcement authorities ("safe harbor"). Also, ISP's must have the protected capacity to remove potentially illegal content from their servers.
- Governments should through education and public in-

formation raise awareness among users of self-regulatory mechanisms such as the means to filter and block content and to communicate complaints about Internet content through hotlines.

Recommendations for the Internet industry

- The Internet industry should develop codes of conduct as a front-line mechanism. Self-regulation of Internet content will enhance user confidence and will increase overall demand for Internet services and e-commerce.
- These codes must be clear and transparent about their policy objectives. In particular, they should delineate the mechanisms through which self-regulation will occur, including provisions for cooperation with end users as well as public authorities.
- Self-regulatory agencies (SRA's) should be created by industry both nationally and internationally to foster the creation and implementation of codes and standards. Such agencies should include a range of content providers as well as service providers.
- SRA's should have a legal structure assuring independence. Important criteria are: institutional stability, composition of the board, links to government, and financial and organizational autonomy.
- An easily accessible, impartial and independent body or agency to hear complaints and adjudicate on breaches of the code should be created by the industry.
- Internet industry should raise user awareness with regard to self-regulatory content concern mechanisms through appropriate means of information dissemina-

tion (at the time of hardware purchase, conclusion of service contracts, and through public campaigns).

Recommendations for joint action

– A mechanism of quality assurance should be provided to assess different self-regulatory consumer empowerment mechanisms and to act as a proxy for insufficiently informed consumers.

4 Rating and Filtering

Filtering technology can empower users by allowing them to select the kinds of content they and their children are exposed to. Used wisely, this technology can help shift control of and responsibility for harmful content from governments, regulatory agencies, and supervisory bodies to individuals. Thus, at the core of the recommendations for an integrated system of self-regulation and end user autonomy must be an improved architecture for the rating and filtering of Internet content.

A flexible filtering system can help individuals choose what kinds of content they wish to view and what kinds of content they wish to allow their children to see.

A good filtering system realizes several important values: (1) end user autonomy; (2) respect for freedom of expression; (3) a diversity of beliefs and values; (4) transparency;

(5) respect for privacy; and (6) interoperability and compatibility.

First, the filtering system should respect end user autonomy, allowing end users the right to choose whether or not they want to filter, and it should provide end users with meaningful choices that reflect different cultural values and ideologies. Equally important, the system must feature a user-friendly interface that encourages actual use of its features and makes choice a real possibility for the vast majority of end users.

Second, the system should be sensitive to freedom of thought and expression. It should not block pages whose content is unrelated to the criteria used for filtering, and it should not attempt to block pages because they are critical of the filtering system being employed. As a default rule, the system should not block unrated sites unless the end user specifically requests this option.

Third, the system must be sufficiently versatile to be compatible with a wide diversity of cultures and ideologies, and it must be flexible enough to change over time as values change.

Fourth, the system should be transparent for end users, raters, and programmers. End users should know when access has been blocked and why. Raters must be able to understand the substantive meaning of different ratings and easily apply them. Finally, information about all aspects of the ratings system should be public so that programmers can create new implementations of the ratings system, and others can easily build on their work.

Fifth, a good filtering system will respect privacy. It will not facilitate collection of data about the filters a particular person is using when they surf the Internet.

Sixth, and finally, filtering software should allow different ratings systems to "talk to each other" and be applied seriatim or in combination. End users who can use different systems together have the greatest degree of freedom in constructing a filter to suit their particular needs.

To achieve these goals, we recommend a "layer cake" model[2]. Our model consists of three layers placed over a software specification. The "plate" on which the system rests is the PICS[3] software specification, including PICS-Rules, and (eventually) the RDF[4] specification.

Our solution relies on a division of labor between first and third parties. We ask first parties (content providers) to describe their content with a standard set of vocabulary descriptors, using terms that are likely to lead to convergent practices. We are less concerned with whether the vocabulary descriptions are value-free (an impossible goal in any case) than with whether most first parties will apply them in roughly the same way. The goal is not ideological neutrality but predictable convergence in behavior. One might call these descriptions "objective" but a more accurate term would be "intersubjectively convergent." This basic vocabulary constitutes Layer One of the system.

We then ask third parties to produce "templates" that combine and rank combinations of these content descriptors in ways that match their particular set of values and beliefs. A template takes the raw materials of content description and then combines them into different categories

2 Illustration as Appendix III

3 PICS = Platform for Internet Content Selection (Labeling protocol developed by the Word Wide Web Consortium)

4 RDF = Resource Description Framework

and decides which combinations are better and worse with respect to a given value system. We do not ask third parties to be ideologically neutral – indeed, we specifically ask them to rank certain types of content based on their values about what is good and bad, and what is more or less harmful to children. The goal of third parties in the system is to set up basic standards of evaluation that will be applied to the convergent descriptions of first parties. Because the basic task of third parties is to set up ratings templates, they do not have to rate sites individually. These ratings templates created by third parties form Layer Two of the system. An end user's browser will read the vocabulary elements in Layer One and filter them according to the templates in Layer Two.

Because ratings templates will be relatively simple and easy to set up, we expect many different organizations will be willing to create them. Moreover, because the templates will be publicly available, organizations can model their efforts on previous templates, making the costs of template creation even smaller. Finally, because all templates will be based on a common language, end users (or other organizations) can mix and match them to produce custom templates suitable to their ideological tastes.

The third layer of the cake consists of ratings of individual sites that can be added to the results of Layers One and Two. Such ratings might include a "white list" of acceptable sites (for example a list of news organizations) provided by third party raters. Layer Three can also contain blacklists of forbidden sites, and, indeed, any other PICS compatible rating system. The purpose of Layer Three is to allow third parties to offer more contextual judgments of individual sites to fine tune the system. While we think that

Layers One and Two offer more diversity than any previous rating system, the addition of Layer Three should greatly enhance the system's flexibility.

End users can install (or have others install) any combination of templates in their browsers. They can also add any combination of PICS compatible filters and whitelists. As a result, even though web site operators use a single Layer One vocabulary, end users can choose from many different and powerful filtering systems.

This proposal features several different layers and many possible options for innovation. But ease of use is not inconsistent with a system that is both flexible and powerful. It is important to distinguish between the complexity of the *filtering system* and the complexity of the *user interface*. A car is an extremely complex piece of machinery under the hood, but its user interface is designed to make it easy to drive. Software companies spend millions of dollars a year to make their user interfaces easy to use despite the complexity of the underlying software engines. We see no reason why this expertise cannot be adapted to filtering, which, in many ways, involves a much less complicated piece of software.

Users should be able to have templates and white lists installed when they first purchase their home computer. They should also be able to click a button on their browser and be taken automatically to places on the Internet where they can download new templates and whitelist updates with a few clicks of a mouse. All of these operations can be made easy and efficient with good software design.

Recommendations for governments

- Governments should recognize that privately created and privately maintained filtering systems can promote individual autonomy, and respect freedom of thought and expression while protecting children. Governments should encourage the use of these filtering systems as part of any scheme of self-regulation.
- Governments can encourage the creation of filters through, for example, tax incentives. However, governments should not impose criminal sanctions for failure to rate web sites, and they should not filter content upstream without the knowledge or consent of individual users. Government should work as a facilitator of private filtering initiatives.

Recommendations for the Internet industry

- Content providers worldwide should be mobilized to self-rate and label their content.
- Members of the computer and telecommunications industries should promote the adoption of a flexible filtering system along the lines of the layer cake model described in our report. Such a system should be incorporated into browsers, search engines, and web authoring tools.
- Industry should promote the availability and use of filtering systems, educating consumers about how to filter and making it easy for parents, teachers, and other concerned adults to choose filters, install, run, and alter them.

– Software design should promote ease of use for end users. Software designers should create easy-to-use interfaces and "wizards" so that end users can quickly and simply install filters and revise filtering choices.
– Endusers should also be able to quickly and easily add particular web sites to lists of approved or disapproved sites. The ability to install filters or alter filtering choices should be prominently displayed on the browser toolbar and not hidden several layers deep in browser menus.

Recommendations for a non-profit rating organization

A The advisory board

– There should be an independent organization to create the initial basic (Layer One) vocabulary elements for the system and to oversee updates to the system at periodic intervals. This organization should be nonprofit and not under the auspices or control of any particular business organization.
– The advisory board should comprise a broad range of expertise on rating and filtering issues. Responsible for creating the initial Layer One vocabulary, it should also create easy-to-use questionnaires to facilitate self-rating by first parties, and easy-to-understand guides for the creation of templates by third parties.

B Other organizations

- Other organizations should be encouraged to create ratings templates for Layer Two that reflect their values and concerns.
- Other organizations should be encouraged to pool their resources to create Layer Three whitelists. These whitelists would include sites that are permissible for children to view (e.g., news sites) even though they might otherwise be filtered (for example, because they contain descriptions of violence). Whitelists create better incentives for cooperation and synergy between non-profit organizations than blacklists, because groups have incentives to spread and share information about sites that they believe are acceptable for children.

Recommendations for end users

- End users should demand easy-to-use filtering from software and hardware manufacturers that puts choice in their hands rather than in the hands of others.
- End users should take whatever steps they can to learn about filtering options available to them.

5 Hotlines as Content Concern Mechanisms

The term "hotline" characterizes organizations ensuring communication from users about Internet content they find of significant concern. Such communication can take place by phone, fax or e-mail. The connection is usually qualified by easy accessibility, high availability and an assured response. We know of hotlines in the private sector where enterprises offer direct access to "help desks" or related services dealing with consumer and client requests.

Hotlines also ensure that an evaluation of content concerns takes place and that effective action can be taken to remedy such concerns. In this context, hotlines are the organizationally supported link between users, content providers, self-regulatory bodies, organizations providing rating and filtering services, and law enforcement. "Content concerns" may range from a merely passing personal irrita-

tion to confronting illegal content. Hotlines have to be open and *not* restricted to criminal law issues like child pornography. On the other hand, they certainly must not exclude these issues.

Mechanisms maintaining and enhancing the communication function of the Internet can be a very effective way to respond to content concerns not sufficiently addressed through filtering mechanisms. In order to function, communication channels need an environment and operational rules that honor procedural and substantive values.

Hotlines have to be perceived as integral parts of content concern response systems and should be implemented and operated accordingly. In particular any procedures developed for their operation should not only take into account the legal obligations of handling sensitive material but the basic rules of substantive and procedural due process, as well as data protection and freedom of expression rules. Hotlines have to fulfill three basic requirements: they must be available, transparent and reliable.

Recommendations for hotline operators

– Hotlines have to be available. The general public must be made aware of their existence. Their availability has to be widely publicized on the Internet as well as in traditional mass media. Therefore, points of mass entry on the Internet (portals, content providers) should contain links to such systems. It should be ensured that linguistic barriers of access to hotlines are either minimized or compensated for. There should be several media available to access hotlines (e-mail, physical mail address,

telephone/fax). There should be a first response to users within 24 hours. If operated automatically, an organizational backup should be maintained to ensure human response.

– Hotlines have to be transparent. Users should be aware – at the point of entry – of the persons/organizations responsible for running the hotlines system and those persons and organizations on whose behalf hotlines are operated. Transparency also means that the rules and procedures according to which concerns are being processed are explained at the point of entry: e.g. which concerns will not be processed; which concerns will be handed over, when, under what criteria and to which public authorities. The system should be explained in sufficient detail and additional help should be available.

  Users should have the ability to track their concern throughout the process and they should be informed of the final outcome of the process. To this end, hotline operators should be informed accordingly by public authorities so that they can provide this information. Organizations running hotline systems should, at regular intervals, make publicly available reports on the basic statistics and experiences with their systems.

– Hotlines have to be reliable. Hotlines have to be part of a technically and organizationally reliable and sustainable infrastructure. Organizations should be aware that they have to dedicate appropriate resources to such systems. Processes should be designed and applied in a manner that ensures that the legitimate interests of the parties concerned in these processes are adequately recognized. The availability and processes of hotlines should be monitored independently. Systems of evaluation, "consumer

information," and quality certification should be encouraged. Hotline systems should have appropriate measures implemented to ensure privacy and data security for their users, including systems by which points of entry to hotline systems can be verified.

– The typical procedure[5] (provided there are no compelling rules that demand a handover to law enforcement authorities) should run as follows:
  (1) The input by the user would be confirmed (information to the user).
  (2) The hotline organization would check the input as to whether the formal point of entry criteria it has set in its policy are met. It would also verify the input as to whether the claimed content concern can be found as described by the user.
  (3) If the (formal) entry criteria are met and verification has been successful, there will be an internal evaluation procedure as to the qualitative criteria with the purpose to determine whether further action is needed (evaluation). This decision-making process will have to follow the criteria prescribed in a policy placed at the entry point of the hotline.
  (4) If this evaluation leads to a decision that no further action is needed, there should be – for reasons of transparency – an information to the user of the outcome.

      If there is a decision on further action the third party has to be addressed. Such a third party may or may not have subjected itself to such an action (within a self-regulative organization). In the latter case

5 Illustration as Appendix IV

the contact merely has the character of a notification. Where illegal content is concerned, a handover to law enforcement may be required.

If the third party has subjected itself to the self-regulatory procedure, it is necessary – for reasons of due process – to give that party a hearing, or the third party may simply decide to take the action requested. A handover to public authorities, as indicated above, might also be necessary – even if the third party responds positively- if there are compelling legal reasons. However, providers subject to a self-regulatory regime that take action according to the requirements should be privileged in a legal proceeding.

(5) Finally, a record of the procedure should be kept and depending on the transparency policy that has been decided the user should be informed of the outcome.

– There should be an international network of hotlines governed by a framework agreement containing minimum standards on the handling of content concerns and stipulating mutual notification between hotlines. The hotline in the country where the content is located should be the entity to evaluate it and to take action. This mechanism results in content providers being acted against only if the material is illegal in the host country. The approach also overcomes difficulties in the complex diplomatic procedures necessary for cross-border cooperation of law enforcement authorities. It is an essential component of an international approach to dealing with content concerns.

– Whether national or international user complaints may also relate to misrating of first parties in the context of

self-rating systems. Hotlines, therefore, serve as back-up mechanisms for the important self-regulation pillar which is self-rating and filtering.

Recommendations for hotlines operated by public authorities

– Public authorities should not hesitate to show presence on the net. Where hotlines are operated by public authorities, they should unequivocally be made recognizable as such, and the legal procedural rules that are followed in their operation should be explained clearly to users.

Recommendations for hotlines operated as cooperative efforts between public authorities and the private sector

– In cases where hotlines are operated in private-public cooperation or under rules of cooperation such rules should be publicized at the point of entry, and whatever consequences such cooperation might have should be explained clearly. In particular possible ambiguities arising from margins of discretion in the handling of notices should be avoided.

Recommendations for governments

– Regulation should formulate minimum requirements on the organizational setup and procedure of hotlines the fulfillment of which should shield hotlines from criminal or civil liability incurred in the proper conduct of their business ("safe harbor").

6 Government Involvement and the Interrelationship Between Legal Regulation and Self-regulatory Mechanisms

Law enforcement is the basic mechanism employed within any country to prevent, detect, investigate and prosecute illegal and harmful content on the Internet. This state reaction is essential for various reasons: It guarantees the state monopoly on power and public order, it is democratically legitimized and directly enforceable and it secures justice, equality and legal certainty. However, a mere system of legal regulation armed with law enforcement would be ineffective because of the technical, fast-changing and global nature of the Internet. In a coordinated approach, self-regulatory mechanisms have to be combined with law enforcement as a necessary back-up.

Recommendations for governments

- There should be no criminal responsibility of mere access and network providers for third parties' illegal content transmissions taking place in real-time through their networks.
- Host service providers merely storing third party content should be held liable only if they have actual knowledge of illegal content, and if a removal of such content is technically possible and can reasonably be expected. The regulation of "notice and take down" procedures should specify the requirements for a proper notification of the service provider.
- Providers party to an enforceable and broadly representative self-regulatory regime, recognized by public authorities, should not be liable for third party content when complying with the requirements of that regime and the decisions of the relevant self-regulatory body.
- Laws should recognize (self-)rating and filtering mechanisms as well as age verification systems to exclude responsibility of providers for content harmful to children.
- It is essential to have adequate legislative powers with respect to computer-based investigations, in particular, adequate powers for search and seizure. It would be helpful to make available a preservation order, which could "freeze" evidence in a fast procedure and thus leave the decision about its delivery to a court judgment. In addition, legislation should be clearer on the obligations of Internet providers with respect to the collection, storage and transfer to law enforcement of data relevant to investigations.

– The power of law enforcement agencies to patrol the net and to act undercover as well as to actively participate in dialogues (chat) with potential perpetrators should be clearly defined and duly limited to ensure effective law enforcement and to protect the privacy of citizens online.
– It should be a top priority to create adequate law enforcement bodies to combat computer crime and illegal content like child pornography on the Internet. This requires attention to all levels of law enforcement, including prevention, detection, investigation and prosecution, and can be achieved by developing centralized units and/or a better coordination of existing competent bodies.

Recommendations to law enforcement

– Law enforcement agencies dealing with computer crime must possess adequate technical know-how in a highly technical and fast changing environment. Training must be comprehensive and on-going.
– When prosecuting illegal content, law enforcement agencies should concentrate their efforts on tracing down and prosecuting the content providers producing or publishing illegal content. Internet service providers and self-regulatory bodies (such as hotlines) should be seen as natural allies in the pursuit of this goal.
– The process of detecting crime and gathering evidence should rely on all legal means and sources available. This should include complaints from users, input from industry and notifications from hotlines. The develop-

ment of efficient trace-back procedures on the Internet should be encouraged.
- Official diplomatic procedures for formal legal assistance should be replaced by more direct cooperation of competent authorities. This could be achieved for example, by developing better communication channels, "focal points" and common databases within law enforcement agencies. International training fora would foster co-operation below the official level and help standardize practices.

Recommendations for the Internet industry

- In order to make codes of conduct enforceable and to move towards internationally consistent minimum rules, codes of conduct should be incorporated into the contracts between Internet providers and their clients as well as into agreements between providers.
- When taking down illegal content, Internet providers should not be over-reactive and instead respect both criminal law and the civil liberties and information rights of their users in order to avoid private censorship and breach of contract. Self-regulatory agencies should provide independent evaluation mechanisms for content concerns relieving providers of such evaluation.

Recommendations for the cooperation between law enforcement and Internet industry

- In many countries, both law enforcement and Internet industry can contribute to better cooperation. Law enforcement should treat Internet providers as potential allies in the fight against illegal content on the Internet. There should be an appreciation on the part of law enforcement of the technical difficulties providers may face in combating illegal content. Law enforcement agencies should ensure organizational transparency to facilitate co-operation with service providers. Service providers should understand that appropriate cooperation with law enforcement is in their interest by facilitating a safe Internet environment for everyone. Internet providers should have a clear understanding of their obligations under existing law.
- There should be a regular exchange of views and mutual training between Internet providers and law enforcement agencies in order to discuss common points of concern, exchange law enforcement know-how with technical know-how, ensure transparency in the relationship and build mutual understanding.
- Internet industry should consider logistical support to law enforcement. This could include:
  (1) creation of focal contact points within the Internet industry, accessible 24 hours for law enforcement agencies and the provision of technical support in appropriate cases
  (2) taking all commercially reasonable steps to verify the identity of subscribers, while protecting subscribers' privacy

(3) the freezing of evidence in urgent cases in accordance with data protection law
(4) advice to users that any posting, transmission, access to and storage, of illegal content may result in removal, termination of service and notification of law enforcement.

– As long as there are no clear legal regulations for self-initiated notifications with respect to serious crimes such as child pornography, Internet providers should consider transferring illegal data to the police without transferring personal data thus giving law enforcement agencies the option to obtain a judicial delivery order. Self-regulatory agencies like hotlines can evaluate content on behalf of providers before data transfer takes place.

7 Awareness Mechanism: Media Literacy and Education

No self-regulatory mechanism can work independently of an education and awareness campaign. The Internet industry working in conjunction with government agencies, where appropriate, should agree to the development of a continuous online and off-line effort to provide general awareness of self-regulatory systems such as filtering systems and hotlines. Such a campaign should be directed at children and parents as well as a general campaign involving society at large. Child-safe sites or so called "fenced gardens" can make an important contribution to introducing young children to the Internet. The culture of self-rating and pluralism in filtering underscores the need for increased media and IT literacy for all ages and a greater role for third party groups involved in self-regulation. Schools should provide the necessary skills for children to under-

stand the benefits and limitations of online information and to encourage greater self-control over problematic Internet content.

8 A Learning System

Technological innovation is a determinative aspect of evolving forms of self-regulation. Therefore, industry and joint industry-government research, nationally and internationally, on the relationship between technology and self-regulation should be intensified. In addition, public debate about the opportunities and hazards of technological approaches to content-oriented self-regulation should be encouraged. Evolving patterns of self-regulation should allow for adjustment to technological innovation.

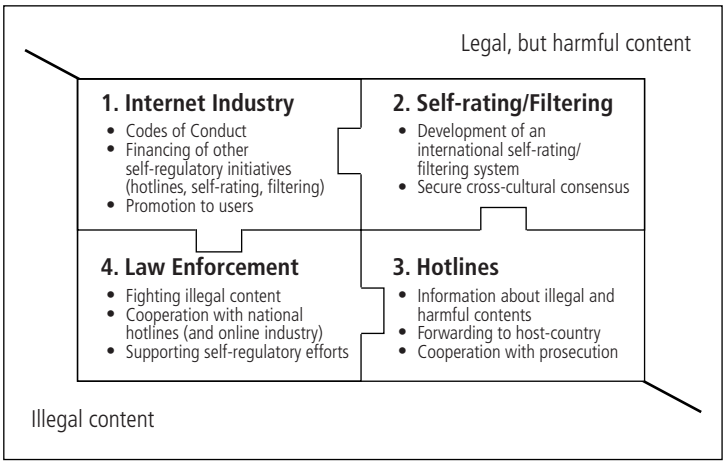
The Internet is, itself, a process, an enormous system for change and response, feedback and transformation. Like the Internet, the legal system and self-regulatory mechanisms around it must incorporate similar practices of learning and changing. The integrated system recommended here depends on continuous (re-)evaluation.

Appendix I

The Bertelsmann Foundation project "Self-Regulation of Internet Content" deals with the problem of harmful and illegal content and the protection of minors on the Internet. Starting from the assumption that no nation-state, no major Internet industry player, nor any law enforcement authority can handle this complex task on its own, the project takes a coordinated approach in four areas:

1. Self-regulation and the Internet industry
2. Self-rating and filtering
3. Hotlines as a feedback mechanism for users
4. Law enforcement and the role of legal provisions in supporting self-regulation.

Figure: International system of self-regulation and youth protection on the Internet



Appendix II

The lead experts prepared reports on four aspects of Internet content self-regulation which were then discussed by the expert network. This document, written by the Bertelsmann Foundation, is based on the lead experts' reports and the discussions of the expert network. Needless to say that not every expert agreed with every point of this document. We nevertheless strived for an adequate representation of the rich and complex discussions.

Lead experts

Jack Balkin

Knight Professor of Constitutional Law and the First Amendment and Director, Project on the Information Society, Yale Law School, New Haven, USA

Beth Simone Noveck

Director of International Programs, Project on the Information Society, Yale Law School, New Haven, USA

Herbert Burkert

Professor for Media and Information Law, University of St. Gallen, Switzerland

Monroe E. Price

Founder and Co-director of the Programme in Comparative Media Law and Policy, University of Oxford, Great Britain; Danciger Professor of Law, Benjamin N. Cardozo School of Law, Yeshiva University, New York, USA

Stefaan Verhulst

Co-director, Programme in Comparative Media Law and Policy (PCMLP), Centre for Socio Legal Studies, Wolfson College, University of Oxford, Great Britain

Ulrich Sieber

Professor and Head of the Chair for Criminal Law, Criminal Procedural Law, Information Law and Legal Informatics, University of Würzburg, Germany

Expert network

Peng Hwa Ang

Associate Professor and Vice Dean, School of Communication Studies, Nanyang Technological University, Singapore

Zoë Baird

President, John and Mary R. Markle Foundation, New York, USA

Stephen Balkam

Executive Director, Internet Content Rating Association (ICRA), Olney, USA

Albert Bischeltsrieder

Detective Director, Bavarian Criminal Investigation Department, Munich, Germany

Rainer Bührer

INTERPOL, Specialized Officer, Economic Crime Branch, Financial Crime Sub-division, Lyon, France

Josef Dietl

Head of Member Relations, W3C Worldwide, Sophia Antipolis, France

Rüdiger Dossow

Directorate of Human Rights, Media Section, Council of Europe, Strasbourg, France

Esther Dyson

Chairman, EDventure Holdings, New York, USA

Clare Gilbert

Vice President, General Counsel, AOL Europe, London, Great Britain

Gareth Grainger

Deputy Chairman, Australian Broadcasting Authority (ABA), Sydney, Australia

Jo Groebel

Director General, European Institute for Media, Düsseldorf, Germany; Chair, Department Social Psychology of Mass-Communication and Public Relations, University of Utrecht, Member of the Council for Culture (Mediaportfolio), Government of the Netherlands, Den Haag, The Netherlands

Ingrid Hamm

Head, Media Division, Bertelsmann Foundation, Gütersloh, Germany

Marie-Thérèse Huppertz

Microsoft Europe, European Affairs Office, Bruxelles

Ekkehart Kappler

Head, IT-Crime Unit, Federal Bureau of Criminal Investigation, Wiesbaden, Germany

David Kerr

Chief Executive, Internet Watch Ltd., Cambridge, Great Britain; Secretary General, Internet Content Rating Association (ICRA), London, Great Britain

Henner Kirchner

Center for European and Middle East Studies, Federal Armed Forces University, Hamburg, Germany; Editor, Middle East Press Digest, Perleberg, Germany

Akio Kokubu

Executive Director, Electronic Network Consortium, Tokyo, Japan

Ling Pek Ling

Director, Policy and Planning, Singapore Broadcasting Authority, Singapore

Marcel Machill

Director Media Policy, Bertelsmann Foundation, Gütersloh, Germany

Ira Magaziner

President, sjs Inc., Boston, USA

Elke Monssen-Engberding

Chair, Federal Media Examination Board for the Protection of Children from Illegal and Harmful Content (Leiterin der Bundesprüfstelle für jugendgefährdende Schriften), Bonn, Germany

Eli M. Noam

Director, Columbia Institute for Tele-Information, Columbia University, Columbia Business School, New York, USA

John B. Rabun

Vice President and COO, National Center for Missing and Exploited Children, Arlington, USA

Jim Reynolds

Former Head of the Paedophilia Unit, New Scotland Yard, International Paedophilia Consultant, London, Great Britain

Michael Schneider

Chairman, Electronic Commerce Forum (eco e.V.), Hennef, Germany

Nadine Strossen

President, American Civil Liberties Union (ACLU); Professor of Law, New York Law School, New York, USA

Richard Swetenham

Directorate General XIII – E2 Telecommunications, Information Market and Exploration of Research, Luxembourg

Jens Waltermann

Deputy Head, Media Division, Bertelsmann Foundation, Gütersloh, Germany

Nigel Williams

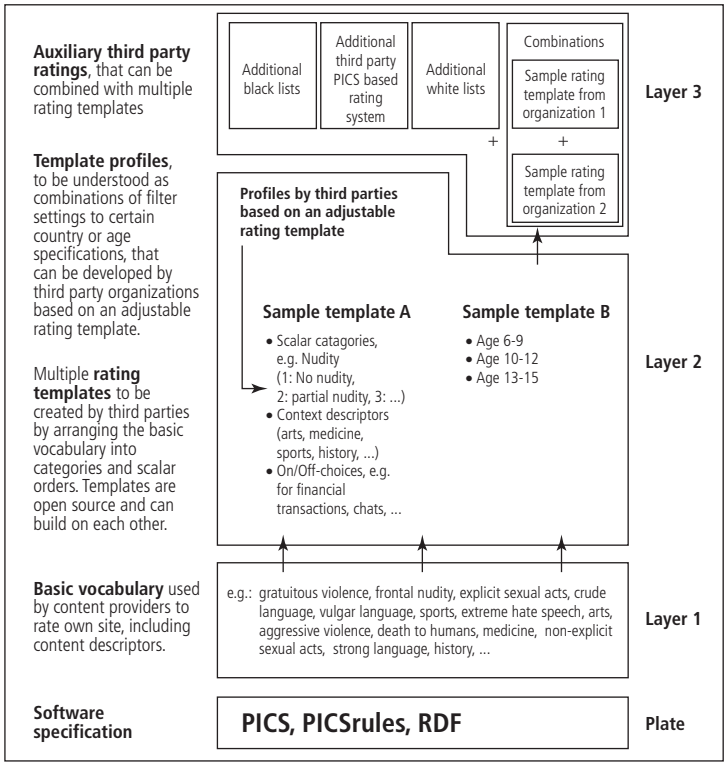
Director, Childnet International; Founder INHOPE-Forum, London, Great Britain

Ted Woodhead

Director, New Media and International Affairs, Canadian Radio-television and Telecommunications Commission (CRTC), Hull, Canada

Appendix III

Figure: Layer Cake Model[1]



1 Rating vocabulary and sample templates for purposes of illustration only.

Appendix IV

Figure: Typical Hotline Procedure