

Speech Control Through Network Architecture

A Public-Private Hybrid

Draft 0.9 June 2004 – Rik Lambers

This draft is intended as a discussion paper for the “Code as Code” workshop, 1-2 July Amsterdam. It is very much a work in progress. Omissions and errors are not excluded. Comments and suggestions are welcome at lambers@ivir.nl .

Contents

	<u>Abstract</u>	
1.	<u>Introduction</u>	4
2.	<u>Networks of Speech</u>	8
	Speech.....	9
	Copying and Print.....	10
	Broadcasting.....	11
2.1	<u>Internetwork of Speech</u>	13
2.1.1	Internet Metaphors and Analogies.....	13
2.1.2	Architecture & Speech.....	15
	End-to-End Design.....	15
	Packet-switching.....	16
	Digitization.....	17
2.1.3	Speech & Architecture.....	17
3.	<u>Nodes of Control</u>	22
3.1	Introduction.....	22
3.2	Physical Layer.....	24
	Lifelines.....	24
	Rights Management: the Broadcast Flag.....	25
3.3	Code Layer.....	27
3.3.1	Ends.....	27
3.3.1.1	Source.....	28
	Geolocation: Yahoo! & Google.X.....	29
3.3.1.2	Destination.....	34
3.3.2	Ins.....	38
3.3.2.1	Source.....	38
3.3.2.2	Destination.....	40
	French Model.....	40
	Pennsylvania Model.....	41
4.	<u>Tilting</u>	44
4.1	Entangled Control.....	44
5.	<u>Conclusion: Fuller on Code</u>	47
	<u>References</u>	51

Abstract

This essay focuses on speech control through network architecture. On how information flows can be controlled through the use of code, where in the network this control may be implemented and by whom. This last question is especially of our interest. We investigate *how the entanglement of public and private regulation of speech on the Internet through its code may restrict the freedom of expression*.

The term *entanglement* refers to the so-called cooperation between public and private forces, and specifically the use of private parties by governments, to enforce public policy. It underlines how after an initial wave of public Internet legislation, followed by a rise of private self-regulatory schemes, the public sector relies on (semi-)private parties to regulate Internet speech.

Translating code, as in law, into technical code proved to be problematic. Enforcement through code does not necessarily include the enforcement of constitutional norms and protections, which define the vertical dimension between state and citizen. By tilting this vertical dimension into a horizontal one, from state-citizen to private parties – citizen, constitutional restraints may be circumvented.

These private parties, notably ISPs, form the “gateways” to the Internet, the new intermediaries in an infrastructure that was initially designed to leave the control over speech to the *ends* in the network. This control is partially moved deeper into the network architecture, regulating the information stream before it may even reach the individual user.

When gateways increasingly function as gatekeepers, the implications for fundamental rights can be troubling. Gatekeepers may become tools of control, and code as their instrument of enforcement. This can collide with freedom of speech on two levels. First, the code itself, the technical enforcement of rules, may prevent users from accessing protected speech or suppress it altogether. Second, the constitutional control on the controllers may be circumvented.

To reach the second level we start with the first. Part of the answer to the question why governments use private points of control, lays in the constitutional problems they have encountered when implementing law into code during the aforementioned first wave of Internet legislation. The points of control and their code-based regulation of speech will be examined in § 3. These form the analytical distillation of the first level, and the basis for a short analysis of the second level in §4. Both analyses come together in the concluding §5, in which the consequences of the intertwinement of law and code, and the entanglement of public and private regulation for the freedom of expression are weighed in light of the Fuller criteria (see Chapter 3). First though, we briefly sketch the framework of our analysis in §1. After that the evolution of speech control (§2) and the network that routes around it (§2.1). Or so it seemed.

1. Introduction

Long before the “code is law” metaphor became fashionable to capture regulation through Internet architecture there was the Panopticon.¹ The Panopticon is code *avant la lettre*. Envisioned by the 18th century British legal scholar Jeremy Bentham as the ultimate prison, it was developed two hundred years later by French philosopher Michel Foucault into a more general model for social control.²

The Panopticon is a reflection of Bentham’s argument for utilitarianism as the driving force in society. In his view the state should not be led by natural rights or a quest for freedom, but strive for the greatest possible happiness: “The right end of all human action is the creation of the largest possible balance of happiness.”³ Morally justified is that which results in the greatest happiness for the greatest part of the population: “(...) the happiness of the greatest number [that] is the measure of right and wrong.”⁴ Bentham rejected natural rights as imaginary and conflicting with the notion of an absolute sovereign.⁵ Instead of freedom thinking he pleaded for utilitarian thinking. In this line of thought the repression of the individual expression can be seen as an acceptable price to secure the greatest happiness for the majority of the people. Individual freedom is not the first priority and subsidiary to the general interest. To serve the majority, the freedom of the minority may be restricted.⁶

To realize this general interest, this greatest happiness, Bentham thought that a government has all possible means of control at its disposal. Of these means the centralisation in an information network is most important. The Panopticon is a concrete example of this centralisation. The word panopticon is derived from the Greek *panoptes*, which means all seeing. It is the probable name for Bentham’s design of a wheel shaped prison with a watchtower as an axis, from where a guard can observe every prisoner at any time without being seen. The prisoner has no anonymity and is made subject to a regime of permanent surveillance, at least the possibility thereof. While the prisoner does not know if he is really being observed at a specific moment, this can always be the case. The result is a regime of one-way transparency, in which the uncertainty and threat of surveillance would bring behavioural conformism to set standards. Control is automatized and enforced through architecture.

Foucault saw in Bentham’s Panopticon more than a model for institutionalized observation and control. Complemented with the concept of discipline he juxtaposed it to the classical idea of power: power as sovereignty. According to

¹ Lawrence Lessig popularized the “code is law” metaphor in his book *Code and Other Laws of Cyberspace* (1999). Joel Reidenberg earlier coined the regulation through network architecture Lex Informatica in his article “Lex Informatica: The Formulation of Information Policy Rules Through Technology” (1998). For an introduction in the “code is law” metaphor see Chapter 3.

² Compare Jeremy Bentham, *The Panoptic Writings*, London / New York: Verso 1995 [1787]. Michel Foucault, *Surveiller et punir, Nuissance de la prison*, Paris: Gallimard 1975.

³ See Muller 1993, p. 190.

⁴ Hart 1982, p. 85.

⁵ *Idem*, pp. 14-15.

⁶ Compare De Hert 2003, pp. 23 + 31.

Foucault this classical idea of power, which determines the sovereign – subject relation, is replaced by a panoptical model in modern societies. Panoptism and discipline govern the mutual relations between individuals and foster the true social control. Foucault presents discipline as a sort of contra-law.⁷ Very generally formulated it is the whole of private methods of regulation of individual behaviour.⁸ The interaction between observation and discipline lead to individual control and form the true power in society. For Foucault the Panopticon was a design of subtle coercions for a future society. It represented a direct and physical power, which people exercised on one and other.⁹

Bentham built his panopticism on the relation state – citizen. Foucault transposed Bentham's panopticism on the relation citizen – citizen. Under the current legal framework of freedom of speech these different relations bring different forms of protection. While the first, vertical relation, is governed by constitutional provisions, the second, horizontal relation, generally is not. This difference is partly seeded in the classical theory of the state and sovereignty.

The relation between the state and its citizens has for long been thought of as a social contract. The people in a democracy collectively transfer their powers to a sovereign so that it may provide order and security.¹⁰ The anarchic state of nature is replaced by the rule of law, enforced by a sovereign government. As underlined by Bentham, the first obligation of the state is to provide security.¹¹ This can be the more general security of the nation, but also the more specific security of groups and persons. In order to secure minors against pornography, groups against hate speech, or people against the infringement on personal rights, amongst which intellectual property rights, the state may restrict the freedom of speech of individuals. The extent of this restriction differs from state to state, but is governed by constitutional restraints worldwide.¹²

There is a delicate balance between the provision of security and the protection of speech. This balance often shows a tension between two functions of law: the instrumental or utilitarian function and the safeguard or rights function. The first sees on advancing a certain goal: law functions as an instrument to secure minors against online sexual content, for example. The second function seeks to offer a safeguard against the abuse of sovereign power by the state with fundamental rights like the freedom of speech.

Traditionally freedom of speech seeks to offer protection against

⁷ Compare Foucault 1975, p. 224.

⁸ Compare Boyle 1997, II. 3rd paragraph.

⁹ Compare Foucault 1975, p. 211: 'un dessin des coercitions subtiles pour une société à venir'; and p. 226: '(...) la formule abstraite d'une technologie bien réelle, celle des individus. (...) le pouvoir qu'elle met en œuvre et qu'elle permet de majorer est un pouvoir direct et physique que les hommes exercent les uns sur les autres.'

¹⁰ See for example Thomas Hobbes, *Leviathan*, Chapter 10, 3rd paragraph: "The greatest of human powers is that which is compounded of the powers of most men, united by consent, in one person, natural or civil, that has the use of all their powers depending on his will; such as is the power of a Commonwealth [...]". (1651).

¹¹ Also see Reidenberg 2004, p. 3-5.

¹² Compare Smolla 1992. Notably, in the United States in the First Amendment and in Europe in article 10 of the European Convention on Human Rights and International Freedoms.

government restraints on individual expression. This is connected to the aforementioned state – citizen relation, which correlates with the classical concept of sovereignty: the sovereign state, bound by geographic borders, setting rules backed by sanctions for its subjects.¹³ In this concept the abuse of sovereign power by government is considered the main threat to liberty. A view echoed by a first generation of thinkers on the Internet. Very much digital libertarians, they both denounced government regulation of “their” online state, and thought it impossible in the first place, since the architecture of the Internet would not allow it. This also meant a denunciation of the government’s role as a provider of security online and a choice for the anarchic state of nature, which the “social contract” had sought to end offline.

A “second generation” of Internet scholars pointed out that the architecture, the *code*, was flexible and being changed by the introduction of private regulatory schemes.¹⁴ Importantly they observed that online regulation of speech based on code was possible and more powerful and effective than traditional legislation, as its enforcement was also embedded in the architecture and automatized. Professor James Boyle suggested early on that the absence of constitutional restraints in the private sphere could be a motive for governments to stimulate and finance private regulation. This action provides an evasion from the practical and legal limitations, which the state – citizen relation brings along: “Intrusions (...) would occur in the private realm, far from the scrutiny of public law. There are advantages to privatizing the Panopticon, it turns out.”¹⁵

We may discover more than a few of the panoptic characteristics in today’s regulation of speech on the Internet: the centralisation of control in an information network; the automatization of enforcement; a one-way, or at least decline of transparency; the demise of anonymity to serve the legal process¹⁶; the use of architecturally design as a reflection of certain values.¹⁷

However, it is questionable if the “Panopticon” is truly privatized. As some of the aforementioned characteristics are analysed in the coming paragraphs, we will come to ask if it is not more a public – private hybrid that regulates speech on the Internet today. That is, the state using private parties to enforce policies and circumventing constitutional protections of speech in the process. An enforcement through private nodes, which might reflect a move

¹³ Compare Chapter 3, specifically on Austin. In this essay references may be made to Chapter 2 (J.C. Fischer, *Code and Technology*), Chapter 3 (L.F. Asscher, *Code as Law*), Chapter 5 (B.J. Koops & R.E. Leenes, *Code and Privacy*) and Chapter 6 (N. Helberger, *Code and Intellectual Property Regulation*). All are drafts for the ‘Code as Code’ workshop, Amsterdam 1-2 July, and can be found on the related website.

¹⁴ Notably Lawrence Lessig, *Code and Other Laws of Cyberspace*, 1999.

¹⁵ Compare Boyle 1997, IV. 5th paragraph.

¹⁶ Compare the plea in Europe for a registration of identity, especially in relation to e-mail traffic: ‘This is desirable in accordance with the democratic principle that individuals, while free to express their thoughts and beliefs, should nevertheless be accountable for their actions. The principle of legal traceability should, therefore, be incorporated into national or European Codes of Conduct for remailing activities.’ Communication to the European Parliament (...) 2001, p. 9. Compare <<http://www.fitug.de/debate/9610/msg00157.html>>.

¹⁷ Recently on the panoptics of copyright enforcement on the Internet, see S.K. Katyal “The New Surveillance”, 54 *Case Western Law Review* 297 (2004), pp. 317-320.

towards utilitarianism at the cost of speech rights.¹⁸

The legal question we seek to answer is to what extent the use of private parties by the state contravenes with the current constitutional framework of freedom of speech. Or, to what extent governments can be held accountable for censoring speech through Internet Service Providers? Is it transparent to citizens that speech may be regulated this way? Do they understand the regime that governs them, and do they even have a choice in obedience? Who is the regulative authority, the sovereign, they can challenge, if at all?¹⁹

Before we may come to seek answers to these questions in §§ 4 and 5, we will now first outline the relation between network architecture and speech (§2). After that we will analyse the nodes in the Internet infrastructure where speech may be controlled through architecture, through code (§ 3).

¹⁸ *Compare* Birnhack & Elkin-Koren 2003, in relation to the Patriot Act and US security policy.

¹⁹ *Compare* Chapter 3.

2 Networks of Speech

In early popular and legal essays the words Internet and Revolution were often presented as interchangeable and likely to be connected to each other until the true free and open society is established. A society in which the means of production and distribution were held by the masses and the ubiquitous flow of digital speech would lead to freedom for all. Not the freedom based in consumption choices by individuals, but the freedom brought by a more pure form of democracy. The Internet as a catalyst for the shift of power from institutions to individuals. Power to control the resources of information, to shape the world in our own image, instead of letting our experience be dominated by the vision of the corporate few.

These rhetoric roots of revolution are strong and grow deep in much of the legal analysis of the Internet. Those who have hailed the Internet for its redistribution of power, democratization of speech and source of unseen individual autonomy, have been labelled communists.²⁰ Major businesses that seek strict compliance to their copyrights are said to rage a war, which strangles innovation and the proliferation of speech.²¹

Such political polarization may leave little room for legal subtleties. It shows one thing though: revolution or not, the Internet is an ever influential factor in our legal thinking about the values that underlay freedom of speech, and the rationales to protect it.

There are several rationales for the protection and even stimulation of speech in our society. Free speech is seen as a means to an end and an end in itself. In both cases this end is the truth. Truth reached through the clash of opinions and ideas in a search for the (objective) truth; and the inner (subjective) truth, man's spirit expressed in his speech.

The first is the rationale of the marketplace of ideas, where "the best test of the truth is the power of thought to get itself accepted in the competition of the market."²² Derived is freedom of speech as a tool for democratic self-governance. The market as a public agora, where by wide participation and debate individual truths are formed to a common policy.

The second rationale, speech as an end in itself, sees the freedom to speak without restraint as essential for reaching individual autonomy and self-fulfilment: expression for its expression.²³ This individual expressive freedom is also considered an important factor in the promotion of a democratic culture. A culture defined by each person's ability to participate in the production and

²⁰ For a spin on this labelling, not with little irony, see: E. Moglen, *The dotCommunist Manifesto*, January 2003. Available at <<http://emoglen.law.columbia.edu/publications/dcm.html>>.

²¹ "This is a war being waged by copyright interests who see each opportunity on the Internet as an opportunity to change the meaning of copyright law." Lawrence Lessig, *compare* <<http://news.com.com/2100-1023-272415.html?legacy=cnet>>.

²² American USC Justice Oliver Wendel Holmes, who formulated the marketplace of ideas metaphor in *Abrams v. United States*, 250 US 616, 630 (1919) (Holmes dissenting).

²³ Smolla 1992, pp. 9-17. *Compare* Balkin 2004, pp. 42 + 43 & 50-55 + 61 on the tension between both "truths": emphasis on freedom of speech as democratic tool tends to minimize the importance of speech as self-expression rationale.

distribution of ideas and opinions.²⁴ Later on we shall elaborate on the democratic values of freedom of speech, political or cultural. Now we will look how the aforementioned ability to participate, is related to the networks of speech involved.

The technologies used to produce and distribute information influence the flow of this information in society.²⁵ Control over communication technologies may determine the proliferation of knowledge and is closely related to the balance of public and private power. Communication networks differ in the extent of concentration of and control over the nodes that make up the network.²⁶ Each node may have a distinct function and be of more or less importance to the dissemination of content. Control over the nodes in the network affects the direction and force of information flows. There are various reasons (and justifications) for a certain distribution of this control, be they based in technique or law, or political and market forces. Let us shortly consider several communication networks and their nodes of control.

Speech

First the most basic of all, a speaker who wants to distribute his thoughts to a single listener or audience offline. His communication may be both one-to-one as one-to-many, with a chance of instant feedback. The nodes in this small "network" that control the flow and direction of the information are few. The speaker is both producer and distributor, his vocal cords the instruments to vibrate his thoughts over air. As long as the air is free, and economic and governmental restraints absent, one may subject his voice to the societal cacophony of opinions and ideas. By protesting in a park, spreading God's word on the streets or political campaigning on the sidewalk, for example. The public forum in its simplest form. Individuals can turn away their heads and walk on by, but the speaker's message will get out in the open and has the potential to attract an audience.

A government could exert control over the distribution of the speaker's message by either using brute force and taking him out of the network (imprisonment, violence) or limiting the environment in which he is allowed to distribute his message. The first would be the act of a totalitarian state, while the latter is recognized by the *time, place and manner*-doctrine in constitutional democracies, and especially the United States.²⁷ It may be considered a form of zoning, which, if excessively applied, could create a barricade between the speaker and his audience, making his message unheard. This could conflict with the speaker's freedom of speech rights.

There may be other factors that make it cost-prohibitive to speak at all and limit the dissemination of information. As we will see this prohibition may be greatly diminished by the Internet's reduction of the cost to speak.

²⁴ Balkin 2004, pp. 3-4.

²⁵ Benkler 1998, p. 184.

²⁶ *Idem*, p. 195.

²⁷ *Compare* Shapiro 1999, p. 124 *ao*.

Copying and Print

The impact of the Internet has been compared to the introduction of the linear press by Gutenberg. Not without reason, since both were accompanied by a drop in production costs, an increase in publishers and publications, an expansion of the distribution network and a swelling information flow in new directions. Before the reproductive technology of print on paper, scribes copied speech on parchment. Though both “networks” facilitate the physical storage of speech, there is a great difference in the distribution of knowledge over society each leads to.

In the copying system the control over information flows is highly concentrated in a few nodes. These nodes, the scribes located in monasteries, united both productive and reproductive functions and led to a centralized storage of information. This so-called “monastic knowledge monopoly” not only resulted in a low dissemination of content over society, but also in relatively little variety in the content itself.²⁸ The powers that were, had little reason to exert control over the scribes, since the content they (re)produced generally represented the predominant (religious) world view and was distributed to only a handful of interpreters. This changed with, or better, after Gutenberg's invention of the printing press that used movable type.²⁹

The technology of print increased the production of information, and generated a wide distribution of this information through a network of publishers and outlets. Where a scribe would copy two books a year a printer could reproduce a book a day.³⁰ The nodes of (re)production were no longer the church-controlled scribes, but craftsmen who had commercial incentives to publish a great amount of non-religious, profitable content. As a result not just Bibles became widely accessible, which strengthened Protestantism at the cost of Roman Catholicism. Generally, more diverse information found its way to the public. The information flow reached further *and* was broader than before.

A reaction to this broad proliferation was bound to come. Governments responded with laws of censorship, which concentrated on the printed works themselves and the different nodes in their distribution network: the writer and those who reproduced and distributed the information, both publishers and outlets. To ease identification and prosecution the names of the writer and publisher had to be printed on the title page.³¹ In England an attempt was made to monopolize the right to print and sell books. Only to be followed by a license scheme for publishers.³² By taxing newspapers the cost of publication was raised; government critics were prosecuted for criminal libel.³³

While in some countries initial censorship was less severe, the

²⁸ Benkler 1998, p. 184, on the “monastic knowledge monopoly”.

²⁹ Sola Pool 1984, p. 226: “The censorship that followed the printing press was not entailed in Gutenberg's process; it was a reaction to it.”

³⁰ *Idem*, p. 14.

³¹ Dommering 2003, p. 5. As we will see this practice correlates to contemporary speech control techniques like identification and filtering through labelling.

³² Contemporary schemes of Internet licensing and registration have arisen in Spain and Italy (central registration of website owners) and Armenia (government registration of ISPs). *Compare* Noorlander 2003, pp. 106-107.

³³ Sola Pool 1983, p. 15-16.

constitutional protection of speech and the press took time and struggle to evolve. The framing of the American First Amendment and subsequent litigation is a notorious embodiment of this process. And even with constitutional protections in place (brutal) censorship was never far away. The Nazi book burnings echoed the burning at the stake of French printer Etienne Dolet four hundred years earlier.³⁴ Heinrich Heine is right, in whichever way you read his words: 'Where they have burned books, they will end in burning human beings.'³⁵

Broadcasting

What is considered censorship under the print model has been accepted as a necessary governmental policy for broadcasting. In the United States the technological limitations of radio and television gave rise to a regulatory decision that provided a communication network based on governmental licensing.³⁶ Since the used spectrum was scarce in light of contemporary technology, it had to be allocated to prevent interference of the transmitted signals. In Europe allocation was often more condensed with the creation of national broadcast monopolies, dominating much of the airwaves for a long time.³⁷

The general consensus that there was a scarcity of spectrum culminated in an asymmetry between licensed broadcasters and passive end-users. Alternative uses of the spectrum and the possibility of future solutions to its scarcity were met with reservations that were often more politically and economically fuelled, than founded on a strict technological basis.³⁸

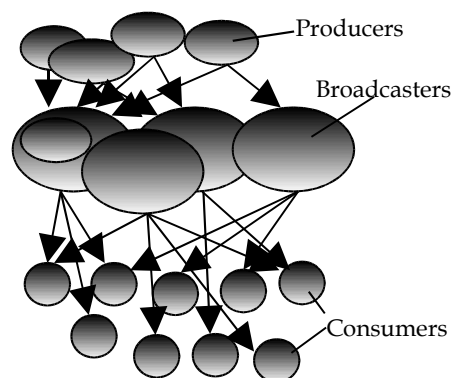


Fig.1 Broadcasting

Production of information became concentrated in a relatively small number of producers and broadcasters, flowing top-down to end-users that had little more control than selecting between the offered channels (see Fig. 1). This concentration was backed by the notion that more broadcasters on a limited spectrum would result in less earnings per broadcaster and therefore in a lower

³⁴ *Idem*, p. 15.

³⁵ Heinrich Heine, *Almansor* (1821).

³⁶ Benkler 1998, p. 187-188.

³⁷ *Idem*, p. 188.

³⁸ Sola Pool 1983, p. 114-116.

quality of the transmitted content.³⁹ An argumentation that momentarily is used in the Federal Communication Commission's (FCC) efforts to protect advertisement revenues of free over-the-air digital television against peer-to-peer file-sharing (see § 3.2).

As said, the nodes in the broadcasting model that determine the dissemination of speech are few and concentrated. The spectrum scarcity, in which this concentration is rooted, has flowered several free speech dilemmas. If few may broadcast to many, and these few are selected on the basis of politically and economically induced criteria, can the government then set regulations for what is transmitted? According to the United States Supreme Court it can: broadcasters' free speech rights may be limited up to a certain level.⁴⁰

Broadcasters are no owners of the spectrum, but licensees. Theoretically they should serve the public interest besides their commercial objectives.⁴¹ Courts in the United States have been inclined to allow the limitation of (offensive) speech to selected hours, or restrict it all together, when the regulatory body of the government (FCC) believed that this was in the public's interest.⁴² These restrictions have been largely met by private censorship.⁴³

New technologies like satellite and cable have partly eroded the scarcity doctrine as a justification for regulation.⁴⁴ Broadcasters have tried to use this technological change to their advantage and support their claim of broad freedom of speech rights, primarily used as anti-regulatory tools.⁴⁵ In analogy with the print model, they have argued that their private ownership of communication infrastructures gives them the right to control the production and distribution of content. An argument that is based on a capitalist theory of free speech, which sees the regulation of telecommunication networks as a restriction on the freedom of expression of the network owners. This is at least questionable, since these networks carry both their own content and speech of others. In case of competition between the two ``freedom of speech`` can mean unrestrained

³⁹ *Idem*, p. 114. + Adding: high production costs - argument

⁴⁰ *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367 (1969), 388: "Where there are substantially more individuals who want to broadcast than there are frequencies to allocate, it is idle to posit an unbridgeable First Amendment right to broadcast comparable to the right of every individual to speak, write or publish."

⁴¹ *Compare* Kranich 2004, p. 5: "The Communications act of 1934 [...] signaled a recognition that government has a role to play in making information available, and set forth a 'public interest, convenience, and necessity' standard for licensing and regulating radio and later TV broadcasting over the public airwaves."

⁴² *Compare* a.o. *Federal Communications Commission v. Pacific Foundation*, 438 U.S. 72 (1976).

⁴³ *Sola Pool* 1984, pp. 119-122 + 135. *Also* Smolla 1992, pp. 326-327. Recently a new wave of self-regulatory action goes through American broadcasting. Time-delay techniques are more widely applied to make the censorship of indecent and violent (live) television possible. A trigger for this wave was the FCC investigation and following policy after the infamous breast flash of singer Janet Jackson during the 2004 Super Bowl.

⁴⁴ *Compare* Lessig 1999, p. 184. Lessig 2001, pp. 76 + 80. Benkler 2000 III, p. 576. The US Supreme Court came close to re-examining the constitutionality of the scarcity rationale in *FCC v. League of Women Voters of California*, 468 US 364 (1984), footnote 11. *Also see*, in relation to cable: *Turner Broadcasting System v. FCC*, 512 US 622 (1994).

⁴⁵ Balkin 2004, p. 31.

personal favouritism.⁴⁶ That is, favouritism towards one's own commercial content above competing content from non-related sources. Freedom to disseminate speech is subordinated to the commercial interests of market institutions. A subordination justified by the capitalist speech theory and which resonates the policies of neoliberalism 'that maximize the role of markets and profit-making and minimizes the role of non-market institutions.'⁴⁷ Inherent in neoliberalism is deregulation of the market so that it can be truly free. It takes to the extreme Adam Smith's view that the natural drive to better one's own condition can overcome the obstructions of law and excessive government regulations.⁴⁸ With the arrival of new technologies media institutions now appeal to law to overcome the regulation of their telecommunication networks.

When it comes to favouritism the Internet has its share (see § 2.1.3). But contrary to broadcasting, its architecture is not limited to a selective and concentrated production of content. Its communication pattern facilitates a much broader division of control and individual autonomy in our society.⁴⁹

2.1 Internetwork of Speech

2.1.1 Internet Metaphors & Analogies

As we saw in the preceding paragraph, communication infrastructures differ in the concentration of nodes that determine the production and distribution of information. This concentration may depend on various factors, interacting with each other and shaping the flow of information in our society. Some are political or economical; others have a technological basis.⁵⁰ Copying on parchment is a costly process, with high concentration of knowledge and little information flow. The technology of print lowered the costs of (re)production and increased the dissemination of information, followed by a political reaction of constraint to the shift of power it provided. Broadcasting regulation has been dominated by the scarcity doctrine and the assumption of high production costs for quality content, resulting in the allocation of spectrum to few producers serving the masses.

Social relations resulting from these incumbent communicative networks tend to be preserved by the institutions, the nodes of control, which provide them and feed from them.⁵¹ They have an interest to sustain the existing

⁴⁶ *Idem*, pp. 24-26.

⁴⁷ McChesney 1999, p. 6.

⁴⁸ Adam Smith, *Inquiry into the Nature and Causes of the Wealth of Nations* (1776), p. 581: 'The natural effort of every individual to better his own condition, when suffered to exert itself with freedom and security, is so powerful a principle, that it is alone, and without any assistance, not only capable of carrying on the society to wealth and prosperity, but of surmounting a hundred impertinent obstructions with which the folly of human laws too often encumbers its operations (...).'

⁴⁹ Benkler 1998, p. 195.

⁵⁰ Lessig distinguishes four kinds of regulators: architecture, law, norms and market. Lessig 1999, p. 87.

⁵¹ Smolla 1992, p. 340.

framework, which is often projected on emerging technologies. For example, while the Internet's architecture greatly undermines the technological and economical justifications of the broadcasting model, it has been interpreted in light of, and fitted into, that structure. Network effects and transition costs from existing to new technologies can create an institutional lock in, which puts the status quo into a perpetual motion.⁵² The approach of new technologies may often be coloured by an old perception. Use of certain metaphors and analogies both strengthens and conceals this.⁵³

"Metaphor structures conception."⁵⁴ If the general conception of communication networks is dominated by the broadcaster – consumer metaphor, the premise for regulating the Internet, may be the aforementioned asymmetrical concentration of production and distribution. A mind set, which at first sight clashes with the Internet architecture, as we will see.

However, many people's earliest thoughts on the Internet were formed by a different metaphor, that of the "Information Superhighway". Injected into the public consciousness over a decade ago it makes certain assumptions about the Internet's nature. Obviously it is a reference to the glorification in American culture of the road as a pathway to personal freedom. That is, the individual transcending the community.⁵⁵ It implies movement, the transfer of information from point-to-point. With super speed and no time to stop. This is not the one-way communicative street of the broadcasting model. Here reign the rules of the interactive one-to-one communication of telephony.⁵⁶ Or so it may suggest and capture the public imagination.⁵⁷

When telephony itself was a new technology courts struggled with the question if they should analogize it to the telegraph and apply its legal regime. While in Britain the answer to this question was positive, the American Supreme Court dismissed the analogy.⁵⁸ Almost a century later, it would again dismiss an analogy, but embrace another at the same time. In *Reno v. ACLU*, the first major ruling on governmental Internet regulation, the US Supreme Court granted the Internet full First Amendment protection. It chose to apply the constitutional regime of the print model, instead of the broadcasting model. This decision was partly based on the rejection of the scarcity doctrine, noting that "(t)he Internet can hardly be considered a "scarce" expressive commodity. It provides relatively unlimited, low-cost capacity for communications of all kinds".⁵⁹

This decision offers an example of how existing law and doctrine is applied on new technologies. From a free speech perspective this print analogy

⁵² Benkler 1998, p. 185.

⁵³ For a broad analysis of the use of metaphors, in connection to law and the Internet, especially the "Cyberspace" metaphor, see: Dan Hunter, 'Cyberspace as Place, and the Tragedy of the Digital Anticommons', *California Law Review* (2003 forthcoming?).

⁵⁴ Moglen 1997, p. ...

⁵⁵ *Idem*, p.

⁵⁶ Blavin & Cohen 2002, pp. 270-271.

⁵⁷ Some also interpret this metaphor as a choice of commercialism above the public good. Compare Blavin & Cohen 2002, p. 270, note 28.

⁵⁸ Sola Pool 1983, p. 100.

⁵⁹ *Reno v. ACLU*, 528 U.S. 844, 22-24 (1997).

may be applauded. Still, it is a generalization of the Internet and reduces a wide variety of applications to a single concept. Not every application is as invasive as the other, or poses equal speech concerns. Junk email, streaming video or web content may provide different considerations when it comes to speech protection.⁶⁰

There are other metaphors, like “Cyberspace as a place”, “the global village”, and even “Code is law”. It is not that these metaphors and analogies have no value, or no basis in reality whatsoever. They can give guidance in the struggle to define the characteristics and legal boundaries of a new technology. But applied on the Internet as a whole they may deny its specific architecture, and diverse possibilities. The Internet should be taken on its own technological merits, and not reduced to some abstraction. When we talk of *the* Internet in the coming paragraph it should be kept in mind that we refer to its general architecture, and not to a certain application per se.

2.1.2 Architecture & Speech

So, what made the architecture of the Internet “perhaps the most important model of free speech since the founding,” as Lessig writes.⁶¹ Notably three important factors contribute to this claim: end-to-end design, packet-switching technology and digitization.

End-to-end design

The architecture of the Internet puts the control over the production and distribution of information in the hands of the end-users, at the ends of the network. This is a result from a specific choice in design, based on what is now commonly known as the *end-to-end-argument*: the intelligence in a communication system should be kept at the ends, in the application-level, while leaving the core of the network, the lower levels of the system, relatively simple.⁶² Simplicity reduces the chance that a device “in” the network fails, which could crash the whole network. Applications, which are “on” the network, may serve more specific and complex functions, because their failure would not have the same impact.⁶³ The core basically only routes the data and is neutral to the applications attached to it. A neutrality which allows technological innovation, the World Wide Web (WWW) being one of the primary examples. Discrimination or differentiation of information flows, associating data with certain applications, has not been coded into the core.⁶⁴ It is too dumb to decide if content is permitted to flow through it, or not.⁶⁵

⁶⁰ Tim Wu makes this point in his “Application-Centered Internet Analysis”, *85 Virginia L. Rev.* 1165 (1999).

⁶¹ Lessig 1999, p. 167. (Referring to the founding of the US Republic and framing of the US Constitution.)

⁶² Saltzer, Reed & Clark 1984, p. 2. (?). Lessig 2001, p. 34. Solum & Chung 2003, p. 14.

⁶³ Blumenthal & Clark 2001, p. 80.

⁶⁴ Solum & Chung 2003, pp. 14-16.

⁶⁵ Lessig 2001, p. 40.

The “e2e” argument, and its exclusion of central control, has been important for the development of the Internet as a platform for a wide variety of opinions and ideas. Instead of a top-down, linear distribution of information, the original architecture of the Internet provided a decentralized and disintermediated network, which transferred potential creativity from the few to many.⁶⁶ The ends turned from passive to active, from consumers to potential users.

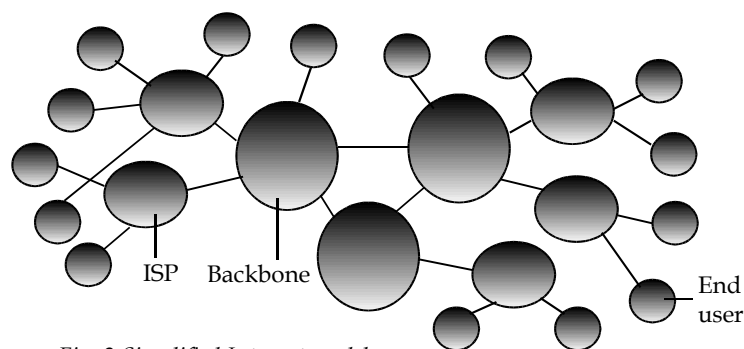


Fig. 2 Simplified Internet model

Where the telephone system is characterized by one-to-one and established mass media by one-to-many communication, the Internet provides both and more. One can send emails, receive streaming video or radio, or publish on a website or Usenet group. Feedback may be instantaneously, establishing an interactive many-to-many communication.⁶⁷ At least in theory, every user has the ability to speak on the Internet, unhindered by a middleman controlling access or editing the stream of words that flows from the ends to the ends.⁶⁸ That on the Internet everyone can be a publisher may prove to be as much a myth as a cliché, will be of later consideration.

Packet-switching

Distribution of information on the Internet is based on packet-switching technology. Information is chopped up and divided over several packets, marked with a source- and destination-address and routed over the network. This is not the circuit-switched linear communication stream of the telephone system, but a diffuse transmission, which was thought to find its way around censorship: “The Net interprets censorship as damage and routes around it.” John Gilmore's famous comment reflected the idea that any attempt to control packet-switched traffic in the network is futile. Where the end-to-end design put the control over production and distribution of content in the hands of end-users, packet-switching prevented the obstruction of distribution. A strong correlation between both architectonic features ensured that users not only could speak in the first place, but also could speak more freely.

⁶⁶ Lemney & Lessig 2000, p. 8. Especially noting the individual innovation the e2e-design promotes.

⁶⁷ Compare Shapiro 1999, pp. 15-18.

⁶⁸ On the negative effects of disintermediation and reliability of information on the Internet, see Shapiro 1999, pp. 135-141.

However, it is nothing but certain that the freedom these features provided will be ensured for the future, or for now. Before the data stream enters the interior of the Internet there may be several points where it can be monitored and controlled. Commercial and governmental incentives have altered the role of online service providers beyond content hosting and basic packet forwarding. Regulation towards served content, and how and if packets are forwarded, becomes more significant. A development that may lead to non-routable censorship, and may be considered incompatible with the end-to-end argument.⁶⁹ In paragraph 3 we will further examine these emerging control points and their influence on freedom of speech.

Digitization

The birth of the Internet is part of what is sometimes called the digital revolution: “the creation and widespread availability of technologies that make it easy to copy, modify, annotate, collate, transmit, and distribute content by storing it in digital form.”⁷⁰

Digitization of information may truly be called revolutionary, as it led to a momentous change in the production, storage and dissemination of content. Digital speech is highly flexible and brings great control over content to the user.⁷¹ It can be pro- and reproduced at very low cost, and is easily and widely distributed without loss of quality.

Combined with the decentralized architecture of the Internet, digitization has led to a massive flow of original, modified and simply copied content. In a sense, digital networking turns the scarcity-doctrine upside down. Where the shortness of bandwidth for broadcast media led to few people distributing information to many, the many-to-many distribution on the Internet, brings a different scarcity to light: that of audience attention.⁷² With the drop in production and distribution costs of speech, and access to a distribution network in the first place, more and more people compete for attention. Attention which requires a more active participation of the audience, pulling speech from the Internet, rather than getting it pushed through their screens. Search engines play an increasingly selective role as a pathfinder in the ever-broadening information flow. As a consequence, those who want to control it, be they public or private parties, will turn their focus on these new intermediaries.

2.1.3 Speech & Architecture

The packet-switched, decentralized architecture of the Internet has been considered an embodiment of the rationales for free speech. Promotion of democracy through free speech is seen as one of its most valuable assets. Ideally

⁶⁹ Blumenthal & Clark 2001, pp. 91-92.

⁷⁰ Balkin 2004, p. 7.

⁷¹ Digital Rights Management systems may offer as much control over content by its producers, right holders, or others who seek to influence its (re-)production and distribution. *Compare* Chapter 6.

⁷² *Compare* Balkin, pp. 7-8.

here rule the end-users, without intermediaries deciding what and with whom to communicate, so it was thought. Since more and more people worldwide get access to the technologies that facilitate unrestrained many-to-many interactivity speech itself is democratized.⁷³ Users are able to participate in the cultural process, once coined in Apple's slogan "Rip-Mix-Burn".⁷⁴ With a dramatic drop of processor and production and distribution costs previous barriers to the marketplace of ideas are slain. Anybody can now express him- or herself and participate in the deliberative process. The net as a huge public forum where each word is weighed for its own value, not the status of the speaker.

As fine an ideal as it is, the democratization of speech does not necessarily enforce the democratic process. Some have warned that the demise of general interest intermediaries on the net may lead to a fragmented speech market. Instead of a package deal including speech with which one may disagree, or simply would not have sought for, one can "select" ones own opinion over and over again. Filtering technologies enable users not to listen to certain speech, or fixate on speech, which is in accordance to their pre-existing worldview. This may only be strengthened by group polarization, websites predominantly linking to websites, which offer this same worldview over and over again, leading to a vicious circle of specific interests.⁷⁵

Filtering has always been a part of our daily life. It enables us to find a path through the massive amount of information, which begs for our attention. Offline filtering is imperfect. Unwanted information will always slip through, confronting us with other people's problems and ideas. A confrontation that is underlays the rationale of speech as a means to democracy: "The cohesion and effective functioning of a democratic society depends upon some sort of public agora in which everyone participates and where all deal with a common agenda of problems, however much they may argue over the solutions."⁷⁶

But even if the entry to this public forum will be unrestricted online, it is questionable if it will flourish and nurture democracy as some have suggested. The perfection of filtering on the Internet, so is warned, can turn our daily life into a daily me: the sovereignty of consumer choice.⁷⁷ On the Internet the marketplace of ideas may truly become a market. One where freedom of speech equals freedom of choice, or better, freedom *from* choice. Individual consumption of fixed ideas rather than stimulation of the democratic process through interaction of opinions.

It is not certain in which direction the Internet develops, though both visions - a filtered world or open society - might be dismissed as dys- or utopian extremes. If individual choice is considered the highest good, reluctant

⁷³ Balkin 2004, p. 10.

⁷⁴ Lessig has underlined this point too great extent, maybe most extensively in his recent book *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, New York: The Penguin Press 2004.

⁷⁵ Shapiro 1999, pp. 105-114.

⁷⁶ Ithiel de Sola Pool. Lessig 1999, p. 180.

⁷⁷ Sunstein 2001, p. 44-46. When it comes to excessive personalization through filtering Sunstein is one of the strongest voices. Not without criticism though, *compare*: http://importance.typepad.com/the_importance_of/2004/01/balkin_on_sunst.html. Also see: A. Chander, Who's Republic?,

of its democratic value, agitating against personalization through filtering can be rejected as a paternalistic interpretation of freedom of speech.⁷⁸ This would be different if government mandated filtering, which could be considered an unconstitutional state intervention with individual speech rights (see § 3). State sponsoring of the development and use of systems of censorship, or the covert use of private parties to achieve public interests is a different question (see § 5).

Democratization of speech is closely tied to the idea that speech on the net is cheap. This may turn out to be somewhat of a delusion. More and more the notion of cheap speech and the effect it may have, the equality of speakers and content, will depend on the used application.⁷⁹

Speech disseminated on the World Wide Web differs from dissemination via email listservs in impact and dependence on the status of its speaker. While on the latter speech may still be weighed for its own value, publication on websites is often determined by the wealth and design skills of the user. Capital does matter, as it buys banner advertisements, supporting software and priority ranking in search engines (see § 3.3.1.1.). The quality of the domain name is of importance to the audience one may attract, as is the linkage by other, popular sites.⁸⁰ And even popularity comes with a price: high traffic brings augmenting costs to sustain the site.

Time, skill and capital are not given to every user. This does not mean that there are and will not be a large amount of “cheap” sites. For example, the WWW is scattered with weblogs, better known as blogs. They provide both diary style personal speech and an exchange of opinions and ideas at relatively low cost. It may be asked though, if their impact does not look pale compared to financially backed, professionally maintained sites.

We should not forget that quantity does not imply quality. More speech is no guarantee for diversity in speech.⁸¹ Cheap speech may truly create cheap speech, in that the amount of messages increases while their content flattens.

The rise of a public agora for all to dwell, takes as a premise that since speech is cheap, users *will* spread their ideas and opinions. But even then the question remains *who* people really want to speak to in the first place, and *how*. It is one thing to have the ability to reach out to the masses, publishing content on the WWW. It is something else to actually do it. Historically people have chosen connectivity over content.⁸² The question is if this will also be the case for the Internet? Will the network be dominated by many-to-many or by person-to-person communications? Again this is a differentiation in applications, which results in a differentiation in speech.

While the WWW may have the potential to influence the socio-political

⁷⁸ Compare Lessig 1999, p. 181.

⁷⁹ Wu 1999, pp.1179-1181.

⁸⁰ The existence of a certain top of highly popular sites may also be an argument against the fear of the demise of general fora. These sites may come to function as collective portals for Internet users, if they don't do so already.

⁸¹ Smolla 1992, pp. 340-341. Noting “The quality of thought does not increase with the ease of transmission.”

⁸² Odlyzko 2000, pp. 2 + 8.

landscape and serve cultural expression, direct communication by email seems to have greater significance to users.⁸³ In the end most people are more interested in social speech. They rather engage in a linear form of informal interaction, than in disseminating speech to a broad audience. Here resonates the choice for individual above communal interaction.

Another example of informal point-to-point communications is file sharing through peer-to-peer systems. It is becoming ever more popular and momentarily dominates much of the legal debate on the Internet. This debate does raise serious issues, as the tension between free speech and copyright, and the values underlying copyright itself. But what are the political values underlying file-sharing, or as the right holders would argue, copyright infringement? Are you really downloading communism, when you pirate MP3s?⁸⁴ Or are you merely consuming large quantities of mostly copyrighted speech? Is every dissemination of every form of speech, commercial or not, an enrichment for our culture?

The point to make here is that people have preferences in speech. Sociability ranks high and affects the value of the applications that support it.⁸⁵ If these are the applications of the future, their flows will be great, but the proliferation their democratic significance uncertain. It shows the need to distinguish between applications and not to generalize speech on the Internet. A generalization that should also be avoided in the code as code-analysis. Regulation of speech through code does not have to bring the same changes for different applications. This is a result of the layered architecture of the Internet (see § 3).⁸⁶ In the next paragraph we will primarily analyse speech control deeper in the network, and distinguish technologies of control with cross-application ability.

Differentiation in information flows not only comes forth from user speech preferences and their related choice for applications. It is also formed by commercial preferences from access providers. Cable companies abide to the end-to-end design, in that every end gets access. However, what kind of access they give is something else, and can depend on their business plans. Favouritism to certain content, speed and applications is not uncommon. File sharing may be the people's choice; some access providers decide to choose for themselves. Data packets identified as related to file sharing are filtered out, because they could compete with other commercial content they provide over cable. Related is the asymmetry between up- and download speeds.⁸⁷ A disparity, which discourages users to create web sites and employ competing web hosting services.⁸⁸ Also a preference for top-down consumerism and possibly conflicting with individual creation and dissemination of content.

Policies of access providers can effectively form a system of control in favour of commercial interests. Control over information flows on their privately

⁸³ *Idem*, p. 9.

⁸⁴ Probable source: <<http://modernhumorist.com/mh/0004/propaganda/mp3.cfm>>.

⁸⁵ Odlyzko 2000, p. 19.

⁸⁶ Wu 1999, p. 1181.

⁸⁷ Benkler 2000 III, p. 575.

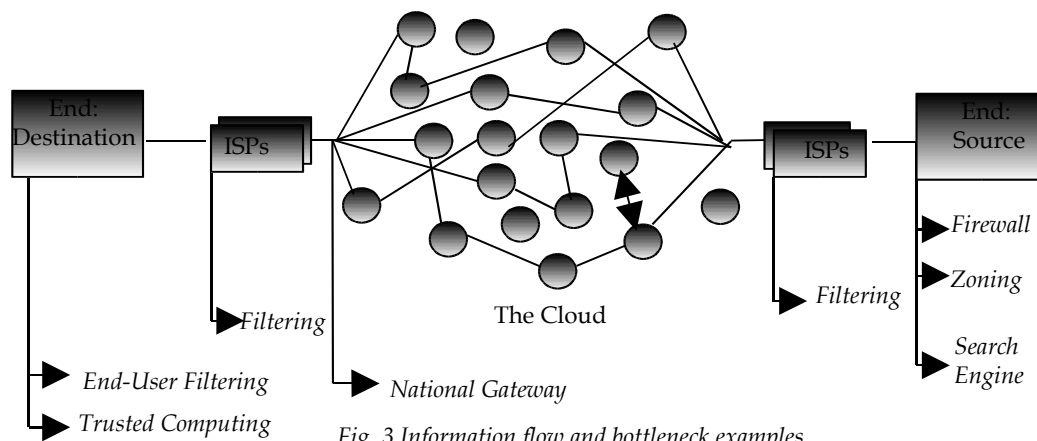
⁸⁸ Lessig 2001, pp. 156-159.

owned physical infrastructure. The capitalist theory of freedom of speech comes to mind. This is very much an area governed by competition law. Though of importance to freedom of speech, it will not be covered in this chapter. Instead we focus on a technical equivalent of the business rules, the regulation through code we already referred to. Employment of technologies to direct, halt and alter the information flow. Technologies that both empower and disempower individual user's control over speech.

3. Nodes of Control

3.1 Introduction

Information wants to be free. This famous aphorism has been repeated like a mantra for the last decades, but the Internet may not move to it. In the end it comes down to the fact that information has little will. Some people want information to be free; others want it to be controlled. Because it is indecent, politically dissenting, a risk to national security, inciting, commercially damaging or infringing on copyrights, to name a few reasons. There is information that not just some, but most people do not want to see free, like junk email and child pornography. Information may want to be “free, as in free speech, not as in free beer”, another famous saying, it is nothing but certain that the architecture of the Internet will generate a flow of information or a flow of “beer” in the future. Beer tasting like spam, to be specific.⁸⁹



Not as much a mantra, but still taken to heart by many people, is John Gilmore's earlier mentioned comment that “The Net interprets censorship as damage, and routes around it.” It also has its roots in the “free and ubiquitous flow”-soil of digital libertarianism, and on first sight finds more fertile ground. When information has been fragmented into packets and enters the so-called Cloud of the network, it is hard to get a grip on them.⁹⁰ The fragmentation frustrates the process of “locking on” to and control information. Packets will ping-pong between the different routers like in a giant pinball machine, bouncing back from “corrupted” ones, and finding a way around to their destination. However, as soon as the information leaves the cloud and is “repacked” to a single bundle, the ping-pong mode changes into a straight shot, finding several bottlenecks on it's path. The flow of information and some of the bottlenecks are illustrated in

⁸⁹ Jack Balkin notes that the “digital revolution” especially decreased the cost of distribution of information. Specifically compared to the cost of receiving information, like spam. *Compare* Balkin 2004 pp. 5-6. For a wide variety of statistics on spam, see for example <http://spamlinks.openrbl.org/stats.htm#received>.

⁹⁰ Blumenthal & Clark 2001, p. 83. + note 26. Also noting that decentralization need not be mirrored in systems that run over it.

fig. 3. These are the points where the code can be (re)written to manage speech.

Gilmore's comment describes the Internet as a body, but does not talk about its different organs: the underlying architecture that makes up the network. If those function to treat censorship as damage, then their sum will lead to a free - as in non-obstructed - flow of information. But as soon as one of the organs functions contrary to the idea of uncontrolled distribution, the information flow can be halted, filtered, or controlled in other manners. To see how and where this control takes place one has to look at the body as a whole *and* at its different components. One has to surgically segment the Internet into its separate, interconnected layers and examine how code may interact with each of them. This layer model, the skeleton of the Internet, has been described in detail elsewhere.⁹¹ We will sustain with a derived division, which fits the Internet architecture in a larger communications system context. Proposed by professor Yochai Benkler it distinguishes three layers, as illustrated in fig. 4: Content, Code and Physical.⁹²

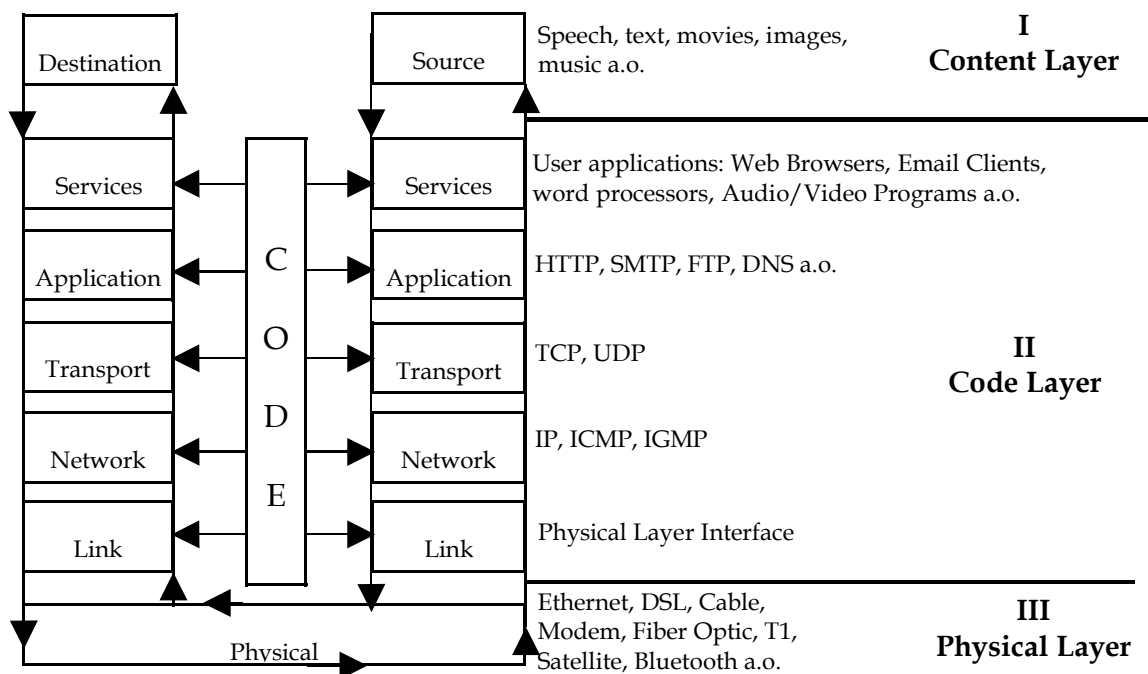


Fig. 4 Data Transport over Internet Layers

At top is the content layer: speech, text, images, movies, music and every other content made available and disseminated on the Internet by its users. This content is transmitted over an infrastructure of computers and the wires that link them together. They form the material basis for communication: the physical layer. In the middle is the code layer: the code, the technical language, which drives the Internet. It consists of the different protocols that form its core architecture and the software upon which they run.⁹³

⁹¹ See Chapter 2.

⁹² Benkler 2000 III, pp. 562-563. Also Solum & Chung 2003, pp. 27-28.

⁹³ Lessig 2001, p. 23. Lessig 1999, p. 89.

Control of content can be achieved through regulation of any of these three layers. What we will see is that efforts to control speech (a Content Layer problem) are often realized through regulation in the lower layers of the network system (the Code and Physical Layer). A discrepancy occurs between the place where the targeted speech is conducted and where it is countered. As control is taken from the ends and moved into the architecture a conflict arises with the end-to-end argument and the principle of layer separation, which brought a transparent, non-discriminatory architecture.⁹⁴ The deeper control is employed, the graver the consequences. Regulation of content at the physical layer can lead to a massive, geographically bound blockade of speech; regulation at the Code network layer (IP filtering) blocks speech from a certain host machine; regulation at the Code application layer (URL filtering) is limited to the speech of a certain document.⁹⁵ Before we shift our attention to the regulation of speech through code, we will pause for a moment at the physical layer. Not as such a part of the Internet architecture, it provides the portals (computers) and wires through which the user may send and receive data. Interference at this level may have far-reaching consequences on access to, and openness of the Internet. We will give two examples of how tampering with the physical infrastructure can undermine the initial values of the Internet.

3.2 Physical Layer

*Lifelines*⁹⁶

The most gruesome intervention in a communication system is to cut its lifelines, the wires over which the information flows. It is as radical as it is rare, and we will give it little attention here.

The wires could be cut both externally and internally. By foreign states trying to isolate another state, or by a state itself, to prevent interaction with the outside world. The first was considered for a moment by the U.S. Government during the NATO war against Serbia in 1999. It had the possibility to cut of a US satellite link, which provided most of the bandwidth to Serbia, but decided against it. The liberal thought was that more outside information would break the state controlled media in the country. The Internet used to route around incumbent information outlets. That most Internet users were anti-Milosevic must have had more than some influence on this decision.

Myanmar, the former Burma, is an example of a dictatorial state that seeks control over the physical infrastructure of the Internet with the ultimate threat of shutting down all communications. While its government has not “cut the wire” to the outside world yet, it has imposed a regulatory regime which effectively provides an axe that can strike at any chosen moment. The only ISP is state controlled, all Internet access is prohibited unless allowed by authorities, every web page created requires prior approval, and contact with the outside world by e-mail or through the World Wide Web non-existent for citizens. Any

⁹⁴ Solum & Chung 2003, pp. 26-27. *Also* Biegel 2001. p. 126.

⁹⁵ Solum & Chung, p. 65.

⁹⁶ *Idem*, pp. 57-61.

violation of this extreme policy of control is severely punished. Virtually the Myanmar government has already cut the wire, but it could do the real thing if it saw fit.

It should be clear that this sort of speech control is as absolute as it comes. Absolute *if* all physical links are truly cut, since it is in the nature of the Internet communication to route around damaged links. Via another cable, microwave or satellite that will bring the message out, or in for that matter.

Rights Management: the Broadcast flag

A recent example of physical layer intervention, and what may be seen as a form of projection of an incumbent network model on the Internet (compare § 2), is the so-called *broadcast flag*.⁹⁷ This technological measure to control the distribution of digital over-the-air television content via p2p-systems blurs the regulation of broadcasting and the Internet. In order to protect revenues from second-market sales and advertisement it expands FCC-protectionism to the ends of the network.⁹⁸

The *broadcast flag* consists of metadata and is transmitted with the digital television signal to “tell” a receiver of these signals whether it may redistribute the content or not. To be effective the architecture of this receiver must facilitate a trusted environment, which can guarantee that the tagged content is only distributed when the broadcast flag allows it. The FCC has made it clear that the broadcast flag will be applicable to any device which may receive digital television signals: “We further note that we intend our redistribution control regulations to apply to any device or piece of equipment whether it be consumer electronics, PC or IT device that contains a tuner capable of receiving over-the-air television broadcast signals.”⁹⁹

If a computer contains a receiver card for digital television signals, the data stream between this card and other applications, and finally the Internet, should flow over a secure channel. The architecture of the computer has to be modified to achieve this, embedding control into the open platform that it is. In result the implementation of the broadcast flag not just restricts the user's (fair use) control over copyrighted content, but also over part of its computer. The FCC tries to replace the red flag of piracy with the broadcast flag, but boards computer hardware and the Internet in its effort.

It may be asked if the implementation of a broadcast flag scheme would

⁹⁷ Likewise, the FCC's adoption of the *Digital Television Orders* in 1997 was based on a commitment to preserve the broadcast model. Benkler 2000 III, p. 572.

⁹⁸ Compare Benkler 2000 III, pp. 569-570. Writing that the “assumption that public discourse is best served by increasing incentives to professional, commercial producers”, even at the cost of individual users, is “a self-fulfilling perception of the world. One starts with an assumption that there are producers and consumers and that consumers are better off when producers have high incentives to produce. One then creates a regulatory system that increases the incentives for commercial production but also increases the costs of becoming any kind of producer, forcing producers to try to recoup these high entry costs by selling to wide audiences. (...) These producers, in turn, make up the political lobby for continuing the basic structure as it is.”

⁹⁹ Federal Communications Commission 4 November 2003, 'Report and Order and Further Notice of Proposed Rulemaking', no. MB 02-230, p. 18. Hereafter FCC Report.

be in line with the right of freedom of speech as given by article 10 of the European Convention on Human Rights and International Freedoms (ECHR).¹⁰⁰ In the *Autronic* case the European Court of Human Rights noted that this right covers the means of reception of information: "Furthermore, Article 10 (art. 10) applies not only to the content of information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information."¹⁰¹ As a governmental mandated restriction of the means of reception and redistribution of content (digital television signals) the broadcast flag should comply to article 10 ECHR. The second paragraph of this article allows a restriction if *necessary* in a democratic society for the protection of the rights of others, amongst which are copyrights.¹⁰² It is this requirement of necessity, which the broadcast flag may not live up to. The regulation is not directly necessary, because the contemporary Internet infrastructure does not provide enough bandwidth for massive illegal redistribution of digital television content. In this light filesharing is impracticable, if not impossible.¹⁰³ The free flow of information has to give way to a preventive measure against potential, future infringements.¹⁰⁴ What is more, a measure that is not the right means to the perceived end. It tries to prevent indiscriminate redistribution on the Internet, but only offers protection against casual copying. The digital speed bump, which is erected for this purpose, does not prevent indiscriminate redistribution. Even if it keeps the average user from doing some casual copying, the one or few individuals who take the speed bump already form a hole in the security regime.¹⁰⁵ This calls the effectiveness and necessity of the broadcast flag in a democratic society into question. Besides, there may be alternative measures with less severe side effects that are more proportional than the broadcast flag.¹⁰⁶

¹⁰⁰ Article 10 European Convention on Human Rights and International Freedoms:

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

¹⁰¹ *Autronic AG v. Switzerland*, ECHR 22 May 1990, at 47.

¹⁰² *Dior v. Evora*, Dutch Supreme Court 20 October 1995, at 3.11.

¹⁰³ Compare Electronic Frontier Foundation, 'Comments of Electronic Frontier Foundation', nr. MB 02-230, December 6th 2002, pp 4-5, at: <<http://www.eff.org/IP/DRM/HDTV/20021206-eff-fcc-comments.pdf>>. Also compare Public Knowledge website: <<http://www.publicknowledge.org/content/introductions/pp-broadcast-flag-dtv-transition/view>>.

¹⁰⁴ The FCC openly connotes this: 'We conclude that by taking preventive action today, we can forestall the development of a problem in the future similar to that currently being experienced by the music industry.' See FCC Report, p. 5.

¹⁰⁵ Compare E. Felten, November 5th 2003, <<http://www.freedom-to-tinker.com/archives/000469.htm>>.

¹⁰⁶ An example is encryption of information at the source. Other possibilities are fingerprinting or watermarking techniques, which do not prevent redistribution as such, but ease tracking down

Overall a mandatory implementation of a broadcast flag regime could run into difficulties with article 10 ECHR. The broadcast flag sets a precedent for the regulation of the Internet architecture, putting third party control over reproduction and distribution directly into the ends of the network. It echoes the private initiatives to implement digital rights management systems into operating systems and software.¹⁰⁷ Governmental support of such systems, and mandating certain standards for those systems, is controversial and Constitutionally suspect to say the least.¹⁰⁸

3.3 Code Layer

Regulation through code is most widely applied, notably at the application and network layer. As we saw there are several Internet nodes that may use code as a regulator in some way (fig. 3). Be they situated at the end (the ends: source and destination) or further into the network (the ins: source and destination ISPs). The core of our analysis will be on the regulation by ISPs in correlation with government incentives to censor speech. Consequences of the entanglement of these private parties and the state will be weighed later on. Before that its overture: the first wave of Internet regulation through legislation, and the self-regulatory wave that followed. Both public and private attempts, mainly considered with the ends in the network. When public meets private we will find ourselves *in* the information flow, with the nodes that may control it: ISPs.

3.3.1 Ends

From the original design of the Internet followed the empowerment of the ends. Decentralization brought redistribution of control over the nodes of production and distribution of speech. No longer the institutional producers, but the users would define the direction and boundaries of the information flow. With an arsenal of applications at his disposal the individual got the ability to both produce and consume speech in vast quantities. Out of this vastness, control efforts have mainly focused on two categories: pornography, and somewhat later copyrighted speech.

In the United States the fear of easy accessibility of sexually tinted images, text and video to children resulted in a legislative cyberspace-opera in three acts: I) the Communications Decency Act (CDA) (1996), II) the Children's Online Protection Act (COPA) (1998) and III) the Children's Internet Protection Act (CIPA) (2000). These are the first fundamental attempts to regulate the Internet to protect minors. Both the CDA and COPA are primarily examples of control of the users environment through zoning at the source (fig. 6). The CIPA used financial incentives, making subsidies to (school) libraries dependent on the

information and its redistribution source. The FCC gives these alternatives some consideration. See FCC Report, pp. 11-13.

¹⁰⁷ Also see Chapter 6.

¹⁰⁸ Compare Zittrain 2003 I, p. 18.

use of filtering systems in their computers, the destination end of the network. Effectively this would turn the Internet into a filtered experience for many people.¹⁰⁹ We will not analyse this legislation and related litigation in great depth, but do give some attention to the technologies that are involved.

3.3.1.1 Source

A natural tendency would be to control the information flow at its source. Dry out the well, so to speak. End the production and distribution at its roots, before it can reach others, who may turn into sources of the prosecuted content themselves.¹¹⁰

Early attempts to stop the distribution of pornographic material to minors were not as much focussed on its eradication, but on isolation.¹¹¹ That is, erecting digital barriers to create a zone unreachable for children. A form of segregation that under the propagated legislation was so restrictive that not just children, but anybody might be refused access by the source. As a “defense” to criminal prosecution for making indecent material available to minors, speakers could implement credit card identification systems or ask for an identification number to verify the age of the user who seeks access.¹¹² Methods that make use of adult identification, instead of child identification.¹¹³ When a child identification system is used everyone gets access to the source, unless it receives a signal that the user is a minor. Such a signal could be transmitted by the browser (service layer, see fig. 4), which is modified by the parents for that purpose and protected by a password.

Zoning with adult identification takes as a premise that nobody gets access, unless the user can prove he is an adult. This turns the burden of proof inside out. Everybody has to show his passport, everybody is suspect. Adults who cannot, or do not want to identify themselves are withheld material that they may lawfully receive. It also puts an excessive burden on the speaker, who has to verify both the authenticity of the offered identification and that his content is covered by the zoning regime. For many non-commercial sites an identification system may be too costly. Individuals and non-profit organisations that, for example, offer information about abortion or (homo) sexuality often miss the funds to maintain the barriers. Rather than speaking, sources might not

¹⁰⁹ Ten percent of the Americans get access through library computers, according to American Library Association, *INC v. United States*, 201 F. Supp. 2d 401 (2002).

¹¹⁰ Note the difference in liability and prosecution of acting as a source of copyrighted content and as a receiver by downloading (destination). This has both a legal and functional side.

¹¹¹ What is considered pornography, and can be regulated or totally stripped from constitutional protections, clearly differs per country. As Lessig & Resnick 1999, p. 395 note: “(...) what constitutes “obscene” speech in Tennessee is permitted in Holland; what constitutes porn in Japan is child porn in the United States; what is “harmful to minors” in Bavaria is Disney in New York.”

¹¹² See 47 U.S.C. § 223(e)(5)(B): [It is a defence to prosecution if a person] 'has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.'

¹¹³ The distinction is made by Lessig 1999, pp. 176-177. For a broad analysis, see Lessig & Resnick 1999.

publish their content due to the threat of criminal liability. Speech gets chilled, because it is not so cheap and could bring grave consequences.¹¹⁴ The United States Supreme Court would recognize this and declare the CDA zoning scheme unconstitutional.¹¹⁵ Another, more current zoning of speech is enforced by so called geolocation techniques.

Geolocation: Yahoo! & Google.X

One of the characteristics of the Internet that seemed unchangeable, that defined its very essence, was its global outreach. A worldwide communication infrastructure, crossing national borders, connecting people from every corner of the planet. All inhabitants of the global village that is the net. However, this structure, this global village might be reduced to a mere national village. Geolocation techniques diminish the hopes or fears for harmonization and global law to some extent. Actually, to quite a small extent for the moment. But over time geolocation is likely to be refined, become more accurate and easier to use.¹¹⁶

Geolocation techniques offer geographic localization by connecting IP addresses to the nationality of a user. Every time a user connects to the Internet his ISP assigns him an IP address out of the block of addresses assigned to the ISP itself. Names and addresses of these ISPs and the blocks that are assigned to them, are stored in a database which is in the public domain. With this information a source can differentiate in content depending on the location of the user. It facilitates the adjustment of language per region and more personal advertising. It also supports the enforcement of local law on foreign soil through code. Blocking of region specific IP addresses at the network layer (fig. 4) will prevent out of state citizens from accessing a source.

An (in)famous example, in which the feasibility of these techniques was researched in order to support a claim of jurisdiction, is the Yahoo! case.¹¹⁷ A French Court ruled that the American company Yahoo! should and could block the access of French citizens to those parts of its auction site that offered Nazi related materials. It based its jurisdiction and the applicability of French law on an effects doctrine: any action committed outside national territory, affecting a French citizen within the national border, may be subject to French law.¹¹⁸ While

¹¹⁴ § 47 U.S.C. § 223(d): [those who fail to comply with the law] 'shall be fined under Title 18, or imprisoned not more than two years, or both.'

¹¹⁵ *Reno v. ACLU* 528 U.S. 844, 28-33 (1997): 'We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.' CDA's partial clone, the COPA, which is limited to commercial speech and is less broad in its scope of covered sexual material, had a bit more favourable hearing by the Supreme Court, but was denounced by a Court of Appeals after referral. *Compare* *Ashcroft v. ACLU*, 122 S. Ct. 1700 (2002) and *ACLU v. Ashcroft*, 99 F. 3d 1324 (2003).

¹¹⁶ *See* Zittrain 2003 II, p.11.

¹¹⁷ *Compare* *La Ligue Contre Le Racisme Et L'Antisemitisme v. Yahoo! Inc.*, Tribunal de Grande Instance de Paris, May 22 and November 20, 2000, No. 00/05308.

¹¹⁸ *Compare* Code Pénal Article 113-7: "French Criminal law is applicable to any felony, as well

the Yahoo! site was hosted abroad on an American server, it could be viewed within in the French borders.

Though Yahoo!'s exhibition of Nazi materials is certainly allowed under American Constitutional law, it is prohibited by the French Criminal Code.¹¹⁹ After the gruesome genocides in the Second World War many European democracies found a restriction on freedom of racist speech justified.¹²⁰ This contravenes with the conception of free flows of information, as established by the American First Amendment and coded in the architecture of the Internet. With some enthusiasm Lawrence Lessig wrote: "We have exported to the world, through the architecture of the Internet, a First Amendment *in code* more extreme than our own First Amendment *in law*."¹²¹ An "extremism" which is not necessarily reflected in the constitutions of other democracies or international treaties. Both the UN's International Covenant on Civil and Political Rights and the European Convention on Human Rights and International Freedoms allow restrictions to hate speech.¹²² The exhibition of Nazi materials can be judged as such.

So, the architecture of the Internet may adhere to First Amendment values, these values are not endorsed by every other country. The allegation that the French Court order to restrict the access of French users to materials, which are rightfully forbidden under French law, threatens the freedom of expression, is based on the premise of certain, American, values. Criticism that the Yahoo! case is a form of European Internet imperialism can be answered with equal rhetoric: the First Amendment was the first to invade European soil. Through the Internet, through code.¹²³

Yahoo! challenged the French decision in American Court, seeking declaratory judgement to prevent its enforcement. Without engaging in an

as to any misdemeanour punished by imprisonment, committed by a French or foreign national outside the territory of the French Republic, where the victim is a French national at the time the offence took place." And Code Pénal Article 113-2: "French Criminal law is applicable to all offences committed on the territory of the French Republic. An offence is deemed to have been committed on the territory of the French Republic where one of its constituent elements was committed on that territory." English version available at http://www.legifrance.gouv.fr/html/codes_traduits/code_penal_textan.htm. Also Reidenberg 2001, p. 5.

¹¹⁹ Compare Code Pénal Article R654-1 (Unofficial translation): Shall be punished by the fine stipulated for violations of the 5th class the fact, other than for the needs of a film; a show or an exhibit enjoying historical context, to wear or exhibit en public a uniform, an insignia or an emblem which evokes the uniforms, insignia or the emblems which were worn or exhibited either by the members of the organization declared to be criminal pursuant to article 9 of the statutes of the international military tribunal annexed to the agreement of London on August 8, 1945, or by a person found guilty by a French or international court of one or more crimes against humanity stipulated by articles 211-1 to 212-3 or stipulated in law number 64-1326 of December 26, 1964.)

¹²⁰ Compare Smolla 1992, pp. 354-356.

¹²¹ See Lessig 1999, p. 167.

¹²² Compare Reidenberg 2001, p 12, note 54.

¹²³ Compare Mailland 2001, p. 1213: 'The European line of cases must be criticized because it has an imperialistic character. It leads to application of one's national law to other jurisdictions and attempts to coerce residents of those other jurisdictions without regard to the laws of and rights provided by those other jurisdictions.'

extensive analysis of the choice of law issue, the American Court applied U.S. Law and found that the French order was impermissible under the First Amendment. It concluded that, while the French State may have genuine reason to regulate speech within its borders, "this Court may not enforce a foreign order that violates the protections of the United States by chilling protected speech that occurs (...) within our borders."¹²⁴

The French and American Yahoo! judgements reveal a general problem of regulating the information flow at the source. If this source is located in a foreign state, the inability of physical enforcement makes a claim of jurisdiction futile. In that sense information is as free as the foreign regime allows. How interesting this jurisdictional question may be, we will leave it for now, and take a short look at the feasibility and consequences of geographic regulation through code.

The French efforts to create a form of zoning through geographic determinism clash with the original ambiguity of the Internet infrastructure towards the origin of data.¹²⁵ Determination on the basis of IP addresses has a 70% accuracy rate, according to the experts' opinion in the French case. This would mean that out of every ten IP addresses blocked seven are connected to computers that are truly located in France. And the other three? Well, it is possible that they are located in the United States, or somewhere else in the world. Some chilling effect might occur for non-French citizens, if they had a right to access the speech in question in the first place.

While the wrongful blocking of 30% of the users could send a chilling breeze over the net, the 70% figure conceals another problem. It is nothing but certain that it has a lasting value, and if, how high that value will be. Nothing in the design of the Internet restrains a reallocation of blocks of IP addresses to a different country.¹²⁶ A user, who's presumed to be French on the basis of an IP address today, may have another nationality in the future. Using IP addresses as the basis for geographic determination leads to over- and under-inclusive blocking, the severity fluctuating with time. Besides, those who really want to obtain Nazi materials through the Yahoo! Site, can use anonymizers to circumvent the IP address blocking scheme. A technology that hides the origin of the user by connecting to the site through another server. It would make it virtually impossible to determine a geographic location. This leads to an under-inclusiveness, which shows that regulation through code is as good and effective as the code allows.

It is argued that the occasional failure of the legal system, its under-inclusiveness, is inherent to a democratic society. Full effectiveness could only be achieved by relying on absolute enforcement. Something, which would result in totalitarianism: a policeman on every corner to control every move, and assure complete compliance with the law.¹²⁷ Maybe this is a benign argumentation, but also one used to marginalize the discrepancy between the normative working of law and its enforcement through code. A discrepancy mirrored in the place

¹²⁴ Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 145 F.Supp.2d 1168 (2001), at 1192.

¹²⁵ See Reidenberg 2001, p. 15.

¹²⁶ See Solum & Chung 2003, p. 81.

¹²⁷ Compare Reidenberg 2001, p. 16.

where the intrusive conduct occurs (Content layer) and where it is sought to be regulated (Network layer in the Code Layer). Sometimes this discrepancy can lead to under-inclusive blocking of speech, but as said, there is another side to the ineffectiveness of the system: those who actually have a right to receive certain speech see this right lost in the absolute enforcement through code. Again, speech control through architecture can be as subtle as one is able to code, to translate, the rules of law into the infrastructure. The problem is that regulation at the Content Layer, through national law, international treaties or other traditional models, is not likely to be effective.¹²⁸ On the Internet code is indeed law and more than often speech has to abide to it.

Efforts to streamline the Information flow to national preferences have not just been limited to enforcement through lawsuits. Outside the judiciary scope, the popular Google search engine has excluded search results on a more informal basis.¹²⁹ Under pressure of local laws, and possibly requests by government officials, Google has proceeded to self-censorship.¹³⁰ There turns out to be a discrepancy between the search results generated by google.com and its German and French counterparts, google.de and google.fr. Again the subject is certain racial speech that is allowed under the First Amendment, but deemed illegal in the specific countries. Searches for white supremacy and related content on the French and German versions of Google were filtered out. The objectionable web pages were removed in a localized post-processing of the google.com database, which functions as the basis of national Google sites. A German or French citizen who uses his local interface will get pre-screened results, probably without ever noticing it. The ranking of search results is already getting less transparent, but this localized exclusion truly turns transparency into invisibility.¹³¹ That is, if one searches with his country specific version. Nothing withholds the user from searching with google.com and avoid the filtering. This might be recommended for most Europeans who seek an unfiltered experience. Because while the google.com site offers to possibility to turn the search engine's filtering system SafeSearch on and off when using the image search function, this choice is not given to several of its derived counterparts. A default of moderate filtering seems to be applied on the search queries, omitting sexual explicit images. Some American puritanism exported abroad.

The filtering in the European versions of Google conveys a more stringent practice. In march 2001 Google removed the links to webpages which contained

¹²⁸ See Solum & Chung 2003, pp. 82-84.

¹²⁹ The localized exclusion of Google search results was first documented in an online report by Benjamin Edelman and Jonathan Zittrain as part of their research of worldwide Internet filtering. See <<http://cyber.law.harvard.edu/filtering/>>. Also see <<http://www.opennetinitiative.net/>> for analyses of worldwide filtering.

¹³⁰ Compare Zittrain 2003 II, p. 11. Also B. Edelman and J. Zittrain, *Localized Google search result exclusion*, October 2002, see <<http://cyber.law.harvard.edu/filtering/google/>>.

¹³¹ The BBC bought up the search terms “Hutton report” and “Hutton inquiry” for the British and American Google sites, so that sponsored links at the top of the page would lead to its online coverage of the report, on the day it was published. A report that was highly critical of the BBC's role in the affair surrounding the death of Dr. David Kelly. The action was described as a marketing strategy and the notion of possible bias waved away.

material that allegedly infringed on the copyright of the Church of Scientology.¹³² The Church tried to make its belief even more unquestionable by invoking the U.S. Digital Millennium Copyright Act to silence criticism to which end the material was used.¹³³ Eager to avoid liability Google decided to ban any reference to the critical site, practically functioning as a tool of censorship.

That online service providers (OSPs) like search engines find themselves in this position, as the possible policing powers of public and private parties, comes forth from both the architecture of the Internet and the law. The architecture provides a technical bottleneck, a point where code can be employed to control the information flow. The law provides a framework in which OSPs are pressured to actually use their powers of control. Over the years a legal doctrine of contributory infringement and indirect liability has been developed in the U.S. If the OSP was aware, or should have been aware of direct infringement by the end-user, and materially contributed to the infringement, he can be held liable if he does not take reasonable steps to control the infringing action after a notice from the plaintiff.¹³⁴ According to the Napster case, reasonable may mean technically changing the system so that future infringement is prevented.¹³⁵ That is, enforcing control through code, moulding the architecture to halt and filter speech, copyrighted or copyrighted and critical of it.

Confronted with possible liability, search engines and other OSPs might be tempted to pre-screen the links they provide, or the content posted on their servers. Even more probable is that they will implement a “notice and take-down policy”, removing content and links after a third party complaint. And this does not have to be restricted to the private sphere. As we will see in greater detail later on OSPs turn out to be an equally attractive gatekeeper for governments (see § 3.2.3.2). They have to take on a role that used to be preserved for the courts, weighing the legality of content and actions. Especially when a public

¹³² See Declan McCullagh, *Google Yanks Anti-Church Sites*, WIRED NEWS, 21 March 2002, at <<http://www.wired.com/news/politics/0,1283,51233,00.html>>. The removed reference was to the website <<http://www.clambake.org/>>. For other examples of DMCA-request removals of links by Google, compare <<http://www.chillingeffects.org/dmca512/keyword.cgi?KeywordID=2>>.

¹³³ A similar tactic was used in the Netherlands, where the Church of Scientology invoked copyright provisions to ban material from the website of writer Karin Spaink. The legal battle that developed recently resulted in a decision by The Court of Appeals in The Hague. It recognized the copyright of the Church, but found that Spaink's publication should be allowed on the basis of article 10 ECHR. Especially since it has an informative, non-commercial character, and the Church of Scientology shows anti-democratic objectives. A rare case in which freedom of information prevailed over copyright. *Compare* Scientology v. XS4all, Court of Appeals of The Hague, 4 September 2003. [check facts]

¹³⁴ *Compare* Birnhack & Elkin-Koren 2003, p. 24.

¹³⁵ See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 2001, at 1021. Recently the Dutch Supreme Court gave its decision in the KaZaA case. Though initially hailed with exclamations as that the Supreme Court had declared the file sharing provided by this p2p-programme legal, a more critical reading does not come to this conclusion. The decision is considered as somewhat of an anti-climax after long road of litigation. The Supreme Court did note that it would likely be impossible to change the programme to prevent all infringing uses. However, it did not answer the question if providing a programme that facilitates infringing use is legal as such. *Compare* Buma v. KaZaA, Dutch Supreme Court, 19 December 2003.

agency is involved, circumvention of the judicial branch should be considered something more than a practical matter. The balance of rights goes astray, as utility overshadows freedom of speech rights (see § 4 and 5).

3.3.1.2 Destination

Control at the destination side of the data flow, at the users' end, has been mainly achieved by filtering technologies. This is content control chosen by the owner of the concerned computer. An individual choice to censor unwanted speech, of which pornography and violence are the main categories. (A governmental mandate of filtering technology is constitutionally suspect, since it would prescribe the censoring of speech one may have a right to receive.)

The rise of filtering software got a boost after the aforementioned public attempts to regulate the Internet. The government and private industries supported enthusiasm for these techniques as a self-regulatory alternative to state control.¹³⁶ It was said to allow end-user autonomy, resonating the end-to-end argument. This was technology that would empower the individual to decide for himself whether to filter intrusive speech.

At least for second generation filtering systems this argument could be made. The first generation methods used text filtering through string recognition, which appeared to be quite crude and lead to an over- and under-inclusive selection.¹³⁷ In addition they depend on blacklists (censored sites) and white lists (allowed sites), composed by trusted third parties, which is a bit of a euphemistic denotation. Five hundred years ago the pope was the trusted third party and the Index Expurgatorius his black list. Now the trust has to be put in commercial companies, which prevent the disclosure of what is actually on their lists with intellectual property and trade secret law. Secret indeed, and non transparent not just for the sake of commercial protectionism. Blocking has more than once been influenced by political motives and shaky norms.¹³⁸

The second generation filtering system promised norm neutrality. And it delivered: a neutrality that does not make a distinction between content that may be harmful to minors *or* to governments. What began as an initiative to offer a private alternative to public censorship could become one of its tools.

The World Wide Web Consortium's Platform for Internet Content Selection (PICS) offers a standard for metadata. It provides information on

¹³⁶ See ACLU 1997, p. 99.

¹³⁷ String recognition filtering searches for the presence of specific words on a web page, such as sex, violence, gay, porno or XXX. When a page contains one of them it is blocked. It is based on quite a crude evaluation, which does not consider context or subtleties of syntax. This results in the blocking of sites like marsexpl.htm, essex.gov or any word that contains sex (sexton, sextet etc.).

¹³⁸ In the past CyberPatrol has blocked the censorship archive of the *Electronic Frontier Foundation* and Usenet groups like alt.feminism and soc.feminism. See American Civil Liberties Union 1997, p. 218. SurfWatch filtered all *Reuters Associated Press* articles on AIDS. See Heins 2001, p. 2. When a subdivision of pathfinder.com created a search engine that enabled users to look up which sites CyberSitter put on her blacklist, the company responded with blocking 150 000 pages of pathfinder.com. Compare http://www.peacefire.org/censorware/CYBERSitter/blocked_com.shtml.

information. With PICS a set of data can be inserted in the metafile of a web page, describing, for example, that this page contains a picture and that this picture shows a breast. Not that this picture is mildly erotic or outright obscene, a judgment which is left to a rating system. Using PICS' neutral description it gives a rating to the page, which can also be implemented in the metafile. On the basis of this rating the filtering system of an end-user may decide if the page is to be blocked or not.

PICS works at the Application Layer of the Internet architecture (see fig. 4). The filtering is done on the URL of a specific page and each blockage sees on one page at a time. It should be pointed out that this is quite another kind of filtering than the IP address filtering at the Network Layer. We saw that this technique was used in combination with, but not restricted to, geolocation, which is focused on the exclusion of certain end-users by the source. It also works the other way around, blockage of the source by end-users. Or ISPs, as we will see. Filtering at the Network Layer will block all data on the site connected to the IP address, not just a specific document. This makes it inherently more under- and over-inclusive and influences the transparency of the Internet to a greater extent.¹³⁹

The idea of PICS was that its neutrality would allow the emergence of a variety of rating systems, each serving the norms and preferences of a specific group of users. For example, a religious group could use it to label content as in accordance or not in accordance with its teachings. A surfing member of this group would not have to worry that he, or his children, would be confronted with objectionable worldviews.

By far the most well know rating system is RSACi.¹⁴⁰ It tries to achieve objective ratings unconnected to an ideology or set of values so that any person can use it worldwide. At least, that is what it is supposed to do. Several factors make it a lot more subjective and culturally biased than its creators might want to admit. This comes forth from the choices made towards the categorical division of speech: its place on the ladder of severity, and thus change of getting blocked. Besides, it will be the providers of the content, the creators of the web pages, the individual users, who have to do the rating and implementation of the labels in the metafiles for the different systems.

As we saw, the first generation filtering systems made use of third parties to compose black and white lists. It led to little transparency of what was being blocked and proved to be an impossible task in the first place. No organisation has the capacity to review even a tiny fraction of all available web pages. The result is that the overwhelming majority of content will never be judged, and blocked when the user adjust his filtering system as such. Since it is the function of this kind of filtering software to protect children against harmful material, most parents who actually use it will choose for this extreme option. The information stream will dry up to a mere creek. A creek that will mainly contain the most popular sites, because third parties have a greater incentive to label

¹³⁹ See Solum & Chung 2003, p. 64.

¹⁴⁰ RSACi stands for Recreational Software Advisory Counsel for the Internet. The name lingers on, but in 1999 the organization enveloped in the Internet Content Rating Association (ICRA).

these than individual non-commercial sites.¹⁴¹

In general organisations like RSACi prefer self-labelling above doing the Sisyphus-labour themselves. This will surely lead to mixed judgements about relatively similar content, compromising the objectivity of the system. It also puts a burden on the freedom of speech. First-party labelling, as it is called, demands that a content provider rates his speech to someone else's criteria. According to American jurisprudence free speech also entails to refrain from speaking. To require an individual to make a statement (labelling) that he would otherwise not make, or to associate himself with norms and values which are not his own, may contravene with this.¹⁴² To invoke a derived constitutional right against a private party has little if no effect, though. As has complaining about the costs a self-labelling scheme imposes on the user. Many individuals or non-profit organisations have little time or money to rate every other page on their website. Few may contain sexual depictions or violence, but all have to be rated and labelled to prevent them from being filtered. Putting the burden, the cost of censorship, on the shoulders of the end-user clashes with the original character of the Internet. Self-labelling is another factor that raises the cost for speech distribution by end-users. Of course a number of the small, non-commercial content providers will be able to label their sites. But many do not have the means to do this, while there are a lot of platforms for alternative ideas and visions amongst them. Great commercial entities generally do have the means to label their content. Content that is largely focussed on a mainstream audience and does not contain many challenging thoughts. Here plays the problem of pluriformity of speech, or better, the lack thereof.

This is all subtle theoretical talk for a system that seems to have disappeared in the obscure. At first sight PICS was a fine initiative, aside from the more general objections against filtering expressed before. It would bring empowerment of the user and keep censorship out of the hand of the state. Or so it was thought, because until now it has not been much of a success and it is questionable if it ever will be. As a system for end-users, or as a governmental tool, for that matter. Because that was one of the major objections of some scholars. That PICS might empower end-users, but empower governments even more. The system is not just neutral to norms; it is also neutral to the place in the information stream where it might be implemented and by whom. Nothing in the design of PICS restricts it to end-user level applicability. ISPs or search engines, possibly pressured by governments, can just as well implement it. And it may be used to filter any speech, not just the sort that is deemed illegal and unprotected by the freedom of speech.

Even if the state does not intervene in the information stream itself by employing upstream filtering, it could encourage and subsidize the use of such techniques by private parties. The state *could* do this, but may it? When the state has a legal interest in the protection of minors against sexually explicit speech, may it then stimulate the proliferation of a technique, which provides "protection" against any form of speech? Lessig did not think so. He prefers a

¹⁴¹ See Lessig 2001, p. 184.

¹⁴² Compare Weinberg 1997, note 82-86.

narrowly crafted law, which precisely sets the boundaries for speech control, above a technique that might pass the boundaries between constitutionally protected and unprotected speech: “[The state] cannot, that is, push an architecture for filtering that extends beyond these narrow categories. Or at least, it cannot so push when an alternative exists that would achieve the government’s legitimate objective without simultaneously inducing the more general filtering. (...) CDA 2.0 is that alternative. For under CDA 2.0, the only speech that is burdened is Ginsberg-speech.”¹⁴³

Lessig has been extremely critical of PICS. It seems that his critique had its effect on this neutral code tool that may serve all masters for every cause.¹⁴⁴ Little has been heard of it lately.

In Europe there has been a push for filtering technology to prevent state censorship of freedom of speech on a communitarian level. The importance of freedom of speech for a democratic society has been emphasized by the European Court for Human Rights in the *Handyside* case of 1976: “freedom of expression constitutes one of the essential foundations of a democratic society (...) It is applicable not only to information or ideas that are favourable received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the publication.”¹⁴⁵ Fifty years earlier American Supreme Court Justice Oliver Wendel Holmes formulated it pointier: “If there is any principle of the Constitution that more imperatively calls for attachment than any other it is the principle of free thought – not free thought for those who agree with us but freedom for the thought we hate.”¹⁴⁶ It is this idea, that the unwanted or unlikable expression should be protected against the public censor, which has helped the push for filtering and labelling systems by the European Commission. An *Internet Action Plan* (IAP) has been established, which focuses on self-regulation by ISPs and stimulation and facilitation of filtering and labelling software. Large amounts of money are made available to different projects investigating and developing this software for European use.¹⁴⁷

Part of the IAP is the INCORE-project (*Internet Content Rating for Europe*), which has specifically researched first-party labelling and filtering. In a final report on this project the authors conclude: “Existing self-labelling and filtering schemes at their current stage of development do not provide a practical tool for European use. (...) The real practical difficulty, which undermines wider use of the systems, lies with too much content being unlabelled and hence blocked by the *filter*.”¹⁴⁸ Use of RSACi, based on the PICS platform, was found to be unsatisfactory, since it could reduce the information stream to a minimum.¹⁴⁹

Towards self-labelling is remarked that “(...) given a positive campaign

¹⁴³ See Lessig 1998, p. 53-54. With “Ginsberg-speech” he refers to material harmful to minors, as was the subject of *Ginsberg v. New York*, 390 U.S. 629 (1968).

¹⁴⁴ See Lessig 1998.

¹⁴⁵ *Handyside*, ECHR 29 December 1976, (seek reference).

¹⁴⁶ *United States v. Schwimmer*, 279 U.S. 644, 644-55 (1927), (Holmes dissenting).

¹⁴⁷ An overview of current support for filtering and rating systems is available at http://www.europa.eu.int/information_society/programmes/iap/projects/filtering/text_en.htm

¹⁴⁸ Kerr a.o. 2000, pp. 6 + 29.

¹⁴⁹ *Idem*, p. 25.

promoting self-labelling and filtering with adequate marketing to consumers and content providers, commercial pressures will persuade sufficient providers to label content to make a system viable.”¹⁵⁰ It is questionable what commercial pressure will achieve with individual content providers who have no commercial incentive. If *sufficient* providers refers to those who have the means to label, than this idea marginalizes non-commercial speakers on the Internet and their speech with it.

The INCORE-project recognizes the possibility that governments might use a labelling system as a tool of censorship. The push for self-regulation and filtering and labelling system was meant to prevent speech control just this. “We do however argue that there are other, easier ways for them to do so,” the researchers conclude.¹⁵¹ Indeed, there might be, as we will see in the following paragraph. Still, it is questionable how far a state can go in subsidizing the research of a technique, which can be used as a tool for top-down upstream censorship. As said, Lessig thought it to be out of line with our constitutional values. But it may be in line with the state doctrine, as we will investigate in §4.

3.3.2 Ins

From the regulation of speech at the ends of the network, we will now focus on the points of control inside the network: the service providers. It is important to make a distinction in these points between Internet Service Providers and Online Service Providers. An ISP functions as a link between the user and the Internet in general: a conduit passing packets of data. When an ISP also hosts his own or other people’s content on his server, he functions as an online service provider. Where under certain conditions an OSP can be held liable for illegal or infringing content, which resides on his server, a conduit ISP is generally immune for such liability.¹⁵² Earlier we saw how Google, an end-OSP, removed allegedly infringing material under the threat of liability by a private party. Hereafter we will first concentrate on the service provider functioning as an OSP (3.3.2.1) and the related legal regimes of liability. After that we will turn our attention on the service provider as a mere conduit, and the possible pressures applied by the state to regulate the information flow and change his immunity (3.3.2.2).

3.3.2.1 Source

Speech control through service providers may prove to be more feasible than going after a wide variety of individual users. The provider forms a source of sources; a node in the Internet chain where the enforcement of law and code regulation can be facilitated relatively easy. Under legal pressures, notably the threat of liability, service providers can be moved to monitor content and remove it from their servers.

¹⁵⁰ *Idem*, p. 32.

¹⁵¹ *Idem*, p.34.

¹⁵² *Compare* Zittrain 2003 I, pp. 12-15.

The liability of service providers is dealt with in a vertical (US) and a horizontal (EU) fashion.¹⁵³ Under the first, different areas of law are covered by different liability regimes. In the US the Digital Millennium Copyright Act (DMCA) covers liability connected to copyright violations, while the 1996 Telecommunications Act sees on the liability in other fields of law. This vertical approach is echoed in section 230 (e) of the Communications Decency Act (CDA). It provides that the small zone of immunity for liability created under section 230 (c) (1) of the act shall have no effect on intellectual property law, federal criminal law or telecommunications law.¹⁵⁴

The DMCA creates a stricter liability for service providers than under the aforementioned immunity regime. It provides exemptions to this liability, if the service provider meets certain conditions.¹⁵⁵ One of these implements a *notice and take down procedure*: a service provider which expeditiously removes or disables access to infringing material after being notified by the copyright holder is provided a “safe harbour” from damages. This notification procedure has to follow a certain structure, part of which is a process of “counter-notification” to the subscriber who allegedly infringed the copyright.¹⁵⁶ The procedure leaves the final possibility of a court injunction open and tries to ensure that the service provider is not put in the position of a judge over the involved parties. That the availability of such a procedure may not prevent the rise of informal and intransparent notice and take down schemes will be the subject of the next paragraph.

Under the second, horizontal fashion, one regime covers all areas of law. This is the approach of the EU Electronic Commerce Directive, which regulates the liability of service providers.¹⁵⁷ It has been argued that a horizontal approach puts less pressure on the service provider and is more favorable to freedom of speech.¹⁵⁸ Since one regime covers all content, the service provider does not have to monitor the data flow to make a distinction between possible forms of liability connected to different content. However, the European regime of liability does leave more room for state intervention. Member States of the Union may oblige service providers to give information that enables the identification of subscribers, when requested by public authorities. Service Providers may also be compelled to inform these authorities of illegal and infringing material once reported by their subscribers. The Directive seeks to encourage interaction between public authorities and private parties, a form of so-called co-regulation.

¹⁵³ Baistrocchi 2002, Paragraph VII A.

¹⁵⁴ Compare Zittrain 2003 I, p.13. The mentioned section 230 (c) (1) reads as follows: “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” 47 U.S.C. § 230 (c) (2002).

¹⁵⁵ Compare 17 U.S.C. 512 – Section 512 (c) (1) (A) (B) (C).

¹⁵⁶ Compare Frydman & Rorive 2002, pp. 51-52. Also Zittrain 2003 I, p.14.

¹⁵⁷ Council Directive 2000/31 on certain legal aspect of information society services, in particular electronic commerce in the Internal Market, June 8 2000, 2000 O.J. (L 178) 3. *Specifically* artt. 12-15.

¹⁵⁸ Baistrocchi 2002, Paragraph VII A.

Article 14 of the Electronic Commerce Directive sets up a similar regime of liability as the DMCA. However, since the Directive knows a horizontal approach, the regime applies to all fields of law. It also sees on hate speech and defamation, for example. The article does not describe a formal notice and take down procedure, and essentially leaves the procedure of notification to be regulated by codes of conduct.¹⁵⁹ That is, to private agreements between business operators. The lack of a (public) standard notice and take down procedure gives service providers little guidance. Without procedural safeguards they might be tempted more easily to take down certain speech. When notified of allegedly infringing or illegal content they have to make a decision: take down the content immediately, and possibly estrange a subscriber, or face potentially high liability. When making a choice between the two options the loss of a subscriber may seem to be the path of least resistance. Or better, of the least costs. Under the current legal regime the “incentive to take down content from the Internet is higher than the potential costs of not taking down.”¹⁶⁰

If we want to protect speech against wrongful censorship by service providers a transparent and procedural sound notice and take down regime should be set in place. The delegation of speech regulation to private parties should be accompanied by a clear set of rights and duties. And even then the temptation to fall back on informal practices remains, as we will see hereafter.

3.3.2.2 Destination

French Model

France, again, and this time the filtering in the network and regulation of destination ISPs. That is, ISPs processing information from foreign source ISPs. Here we see the first signs of the tilting of the vertical relation between state and citizen into a horizontal dimension. The creation of a private sphere of speech regulation, loosened from constitutional protections.

Before the Internet the French government had some experience with controlling a national technical infrastructure, the so-called Minitel. This is the generic name for a statewide videotex system, with only one access provider.¹⁶¹ As a centralized network it is more open to content control than the decentralized Internet architecture. That did not stop the French government from trying to regulate speech on the net, and soon ISPs stood in the middle of its attention. Two documents outlined a publicly imposed system of private regulation. First, an amendment on the Law on Freedom of Communication obligated every ISP inside France to implement filtering software into the browsers they distributed. It retained from prescribing that these systems should not be turned off, but the government went further. A second document, a policy paper on the information society, calls the labelling of websites essential for the

¹⁵⁹ Neither does the European Cybercrime Convention, nor national laws in European Union.

¹⁶⁰ Ahlert, Marsden & Yung 2004, p. 12.

¹⁶¹ See Mailland 2001, pp. 1188-1191.

successful self-regulation of the Internet by the private sector. That is why the government supports the development and usage of (French) labelling and filtering software. A French label, based on French norms, is supposed to be assigned to information on the net.¹⁶² The next, but not yet mandated step, could be that sites that are not labelled have to be filtered by ISPs. Software to achieve this already exists in the form of PICS. A final goal could be the implementation of a PICS-like system and turn private gateways into public gatekeepers.¹⁶³

The “chauvinistic” code, which threatens to be created with these French labels, has considerable consequences for the information flow inside the country.¹⁶⁴ When a state mandates ISPs to filter on national labels it effectively seeks to keep foreign information outside its borders, and encourages a territorialisation of the Internet. From global to national, from wide dissemination to minimalized choice.

Preventive filtering of information because it is not labelled is censorship. The institution that is engaged with assigning labels a censor. The French policy paper proposed to establish an administrative agency that is responsible for the formulation of rules of conduct, and the monitoring of the ethical conformity of the content distributed over the Internet. So, a central organ that must supervise an extraordinary broad and abstract concept like ethics. In France it is incompatible with constitutional norms to provide such an organ with powers that are not precisely defined by law and have to be exercised without a clear understanding of what ethical conformity may mean.¹⁶⁵

Pennsylvania Model

The destination ISP has the obvious advantage that this node is located inside the jurisdiction of the state which seeks to regulate certain speech. End-users who reside in the state make mostly use of local ISPs, while the sending source may be located outside the state. From a perspective of enforcement it is preferred above trying to exercise control outside the state's boundaries, as would often be the case with source ISP regulation. This last node in the transmission chain, the destination ISP, provides probably the most effective point of blockage for information flowing from foreign soil.¹⁶⁶

On a national level China and Saudi Arabia use the backbone ISPs for countrywide filtering of the incoming data traffic. Just before information may reach users it is screened on prohibited political, religious or sexual content. A scheme that has recently been copied by the American State of Pennsylvania, narrowing the filtered speech to alleged illegal child pornography. At least, that is the goal of the law which provides a specific “notice and take down” system. If

¹⁶² Comparable, the French top-level domain name as (national) hall-mark: ‘Le ‘.fr’ est dès lors perçu comme un espace de qualité respectant le droit des marques, la logique étant celle d’un référencement de confiance.’ Paul 2000, p. 51.

¹⁶³ See Mailland 2001, pp. 1220-1224.

¹⁶⁴ The French government walked this national code road before with the regulation of television. By prescribing a national standard model it encouraged national information flows. See Shapiro 1999, p. 12.

¹⁶⁵ See Mailland 2001, pp. 1225-1226.

¹⁶⁶ Compare Zittrain 2003 I, pp. 19-20, who coined this case the Pennsylvania Model.

a destination ISP is notified by the state attorney general that child pornography is to be found on a certain source, and this notification is backed by a formal order from a state judge, the ISP has to disable access to that source in five business days under threat of criminal penalty.¹⁶⁷ It is interesting enough to see that the apparent immunity of destination ISPs, functioning as mere conduits, is changed with this kind of regulation. If they do not answer to a formal notice and take down they can be found liable for passing illegal content to a source within Pennsylvania.

There are several problems with this scheme. First, in practice the state attorney general made use of *informal* notices and sidestepped judicial review. Local ISPs got requests to remove links to web content the attorney general thought to be illegal, to which they tent to adhere. Second, even with a judge finding that there is “probable cause” that a blocked source contains child pornography, the source is not notified that his material, his speech, is subject to state censorship. He can make no objection to the blocking, and if the blocking is in place it is effectively limitless in time. An IP address, which is blocked today for allegedly containing illegal content, will be blocked in the future. Even if the content changes or the address migrates to another user. This results in a crude approach of speech control, which looks like prior restraint.

It is not just that the source is not notified of the blocking, neither are the users who want to access a certain site. It is not transparent to them for what reasons and where in the Internet data chain the information they request is filtered out. The Pennsylvania government does not, as yet, maintain a list of sites deemed to contain illegal content, making the process of censorship at least controllable.

The techniques destination ISPs use to block certain sites, DNS poisoning and URL routing, bring problems of their own. They can lead to quite a substantive overblocking, censoring speech every citizen has a plain constitutional right to receive.¹⁶⁸ It is the same constitutional problem on which the United States Supreme Court struck down the *Communications Decency Act*. Only now it is hidden in a non-transparent, often informal legal scheme not open to objection by interested parties. A scheme in which a government agency makes use of private nodes of control in the information flow to achieve a public policy. It is not surprising that the first case against the Pennsylvania model of filtering through the destination ISP has recently come before a Pennsylvanian court.¹⁶⁹

The Pennsylvanian model of speech control shows how a government may use a private party as a policing tool. How it may avoid constitutional frictions, which come with prescribing filtering techniques to individual users. How it can bypass jurisdictional problems and concentrate on the most vulnerable node in the Internet chain. *In* the chain, outside the sight of the end-user, making use of a technical tool of enforcement deep in the Code Layer (see fig 4.). A violation of

¹⁶⁷ *Idem*, pp. 21-22.

¹⁶⁸ For a detailed explanation of these techniques see Chapter 2.

¹⁶⁹ Center for Democracy & Technology e.a. v. Michael Eisner, US District Court for the Eastern District of Pennsylvania, No. 03-5051 (2004).

both the end-to-end argument and layer separation.

This practice of molding private power to public use by government has been labelled the comeback of the state, or the persistence of law.¹⁷⁰ Others claim that the state has never even left the scene. In the following paragraph we will try to see to what extent this constitutional scene has been rearranged and what this means for the protection of speech on the Internet.

¹⁷⁰ *Compare*, Birnhack & Elkin-Koren 2003, p. 2. *Also* Hughes 2003.

4.1 Entangled Control

In the preceding paragraph we have seen examples of how private nodes in the Internet chain may control the information flow by using code. This can be done at the ends, with more (end-user filtering) or lesser (search engine filtering) knowledge of the user. It can also be done deeper inside the Internet architecture, by OSPs.¹⁷¹ This may happen under possible pressure of, or after an informal request or an order of a government agency to take action. That is, action against speech distributed or sought to be received by a user, which is a citizen of the state. So, when a state uses an OSP to control speech one public and two private parties come into play: the state, the OSP and the user. From this we can distinguish a state-OSP and an OSP-user relation.¹⁷²

The state-OSP relation does fall under the constitutional protection of speech. When an OSP is unwilling to cooperate with an informal request or order, he may call his speech rights into action. If this call is justified will have to be tested in court, which traditionally has a clear role in controlling state action against the freedom of speech.

A user will find it hard to take the way to court. The classical vertical state-citizen relation on which the current constitutional framework of freedom of speech is founded, is short circuited since a second private party shifts between the state and the user: the OSP.

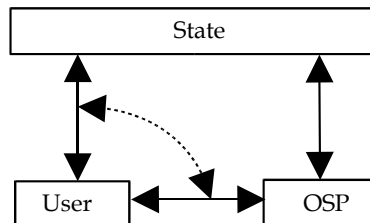


Fig. 5 Tilting

The vertical dimension state-user tilts into the horizontal dimension OSP-user. The first was governed by the constitutional protection of freedom of speech. The second is limited to the rule of private law, and offers no real constitutional protection for the user. A user who seeks to protect his speech rights has little possibility to do so. He has a meagre basis for an action when his web page is blocked or removed, or his requested information is filtered by the OSP. If he discovers that this is the case in the first place, because the regulation through nodes inside the architecture is little transparent. He may fall back on private law and make a contractual claim, if there even is a contract. For speech rights this will not be a very fruitful road. However, he cannot invoke constitutional law against the OSP, and has no direct relation with the state to do so.

¹⁷¹ Here OSPs encompass both online content providers and ISPs in their function as mere conduits of content.

¹⁷² The following is partly inspired by Birnhack & Elkin-Koren 2003, pp. 48-54.

The entanglement of public and private control of speech on the Internet is not a new phenomenon. That is, the difficulty to make a distinction between the public and private spheres and related rights has since long been subject of discussion. Built on the classical concepts of sovereignty and the state this distinction has become a dogma that determines the current constitutional framework of speech.

On this distinction the constitutional protection of speech against censorship by private entities has categorically been rejected. In the United States this rejection is rooted in the state action doctrine, which underlines that the Constitution sees on state conduct. The First Amendment proscribes that “Congress shall make no law [...] abridging the freedom of speech [...]”. *Congress*, that is a body of the state, should refrain from censorship. Non-governmental, private action is literally not covered by the constitutional protection of speech. Likewise article 10 of the European Convention on Human Rights and International Freedoms (ECHR) shields speech against public and not private actors. For those who find their freedom of speech rights restricted by private regulation through code this doctrine may form an insurmountable hurdle to a broader protection.

It cannot be stated that just because online private parties, like search engines and ISPs, have an ever important role as facilitators of public access, they should fall in the realm of constitutional law. A few scholars have condemned this, and reject the public-private distinction as intrinsically incoherent. Invoking some of the Legal Realists theory, they call the existence of two distinct spheres illusionary and propagate the applicability of constitutional norms and values on private code regulation.¹⁷³

While the full application of constitutional rights on the horizontal relationship is generally not recognized, courts have made some rare exceptions. Constitutional law may be invoked when a private party effectively functions as a state agency. This can be the case when the activity of the private party results from the state’s “coercive power” or when the state significantly encouraged the action.¹⁷⁴ To determine if constitutional law could be applied under the state action doctrine the hybrid of public and private forces has to be segmented and analysed. One can argue that OSPs, under influence of legislation like the US Patriot Act, have been encouraged to take action and that this encouragement comes forth from coercive action by the state. The immunity from damages granted by the Act, is certainly an encouragement to police information streams. Something, which until now was a function of state agencies. If the state action doctrine is successfully invoked, the user may fall back on constitutional law against the OSP. On its turn the OSP may however be immune for action.¹⁷⁵ It will be a hard case to make.

States have focussed on the nodes in the Internet chain, which are the most effective tools of online policy. With a number of legislative acts OSPs are pushed deeper into an active role of surveillance and private policing for the sake of national and personal security. Notable examples are the Digital

¹⁷³ *Compare* Schiff Berman 2000, p. 1266. Radin & Wagner 1999.

¹⁷⁴ *Compare* Birnhack & Elkin-Koren 2003, p. 52, nt. 296.

¹⁷⁵ *Idem*, p. 52-53.

Millenium Copyright Act and Patriot Act in America. The former increases liability of OSPs for copyright infringement and widens the obligation to release the identities of alleged infringers. The latter makes use of a legislative good cop - bad cop technique. On the one hand the government may obtain data from service providers with less restrictions. On the other hand the act gives immunity of damages if the providers voluntarily hand over information on the activities of their subscribers.¹⁷⁶ This is a not so covert push for service providers to voluntarily cooperate with government agencies. Avoidance of damages functions as an incentive to control the information stream for the state.

A voluntary cooperation means that users will not be able to sue the government under the state-citizen relationship.¹⁷⁷ The lines between law enforcement by public and private parties blur, while user rights deteriorate. An entanglement of speech control slowly submerges from a legislative environment in which the instrumental, utilitarian function of law gains ground.

Bentham's public panopticon is partly put to practice with a detour via OSPs: private parties that use surveillance on other private parties (users). Panopticism in the private sphere, as Foucault envisioned for a future society.

¹⁷⁶ See Reidenberg 2004, pp. 12 + 15-16.

¹⁷⁷ See Birnhack & Elkin-Koren 2003, p. 51.

5. Conclusion: Fuller on Code

The outset of this chapter was to see what the use of code by private parties, notably ISPs, under more or less influence of the state, might mean for the current legal framework of freedom of expression. What are the consequences for the protection of speech when code is used to enforce certain policies, instead of traditional law? Is the use of code to regulate speech online, as described in the preceding paragraphs, in accordance with certain minimal criteria of (constitutional) law?

In chapter 3 several questions have been asked on the basis of Fuller's criteria for what makes up law.¹⁷⁸ These could be used in an attempt to answer the abovementioned dilemmas. The most prominent dilemmas, concerning the described interrelation between public and private parties, might have to do with the trust in code; the transparency of code; the consistency of the system that code regulation of speech may impose; the reliability of the code; the choice of users to obey the code imposed; and the authority, or sovereign, which applies them and the possible conflict with the traditional legal framework of speech. This is a wide array of questions and we will briefly look at each of them to see whether the speech control through network architecture shows friction with the concept of law derived in chapter 3. Of special interest are the questions if a sovereign can be distinguished who makes and imposes the rule, and if a conflict submerges with traditional legal norms.

The questions if the used code to regulate speech online can be trusted, if the code is reliable as in predictability and if the different forms of regulation through code form a consistent system, seem closely related. All three are somewhat interconnected and the answers depend on the used form of code. A usage that also propels the question of transparency: the ability of end-users to understand what code enforces and to be aware of this enforcement.

As we have seen the blocking and filtering of speech on the net can be achieved by different techniques (URL routing, DNS poisoning, IP address filtering, URL filtering ao) in different places in the layer model (application layer, network layer ao) and by different parties in the Internet chain (end-users, OSPs and ISPs). If one thing, this variety of possible regulation techniques of speech does not contribute to the *transparency* of code as a regulator. It is extremely hard to see for an average user where, how and by whom speech is regulated. Some of the end-user filtering techniques overblock websites with no or little knowledge of the user. Blacklists of third parties are generally not disclosed; PICS based filtering of RSACi labelled sites knows institutionalized preferences of which the user more than often is not aware. The collateral damage of filtering at ISPs may not be transparent both for those whose speech is (accidentally) filtered and the general user.

When speech, rightfully or not, is made unavailable at the level of ISPs, the general public does not know that rules are enforced. It is fairly impossible to be aware of a system of rules, if one does not have the knowledge of its actual

¹⁷⁸ Compare Chapter 3: the essay by L.F. Asscher, *Code as Law*.

existence and enforcement. A related question is if citizens should be aware of the filtering and blocking of speech they did not have a constitutional right to receive or disseminate in the first place. Can one object to the removal of hate speech, if it is excluded from constitutional protection? The problem may be that one does not even come to answer this question, because both the removal and the remover are hardly visible.

The traditional laws that provide a legal basis for the application of filtering or blocking may provide a somewhat *consistent system* with predictable norms. They are formed within a democratic process, and whatever flaws this process may have, it can be checked. The subsequent enforcement of traditional law through code is something else. It can be questioned if there is a consistency in the different forms of code regulation. As we saw there are different techniques to control speech. The choice for either one of these techniques is not directly clear. When an ISP is asked to block or filter certain content he may do this by focussing on an IP address or an URL. As we have seen the first use of code is more precise, but a consistency in this use is not obvious. The doctrine of overbreadth has been applied in Internet related cases, but still there seems to be a lack of consistent system of regulation in this field.

Uncertainty of both the applied code and the working of the code itself do not help the *predictability* of code as a system of regulation. Different claims are made about the effectiveness and preciseness of code, but it still cannot be said to offer a reliable system. In many aspects code regulation of can speech be quite perfect. Sometimes a bit too perfect, in the sense that the regulation is more absolute than desirable. While a certain technique may be applied to enforce a perfectly legal regulation of illegal speech, the result may also encompass the regulation of protected speech. Geolocation techniques, for example, have a margin of error, which may be prohibitively high. A claim that they block speech within acceptable limits, that they are precise enough to be applied as a form of law enforcement, is controversial. At least for the moment, the future may bring more precise tools that do what they are expected to. Some scholars say that imperfections are inherent to every legal system. Just because a law does not prevent every violation, does not make it less legal. But to a great extent this argument is based on a cynical positive: code regulation may not prevent all speech violations, but it may violate more than a few individual speech rights.

Do users have a *choice* in obeying the rules? Do they have an exit out of the system of code regulation? When it comes to ISP filtering users may have some options to look for alternative hosting servers and access providers in a competitive market. Different providers may bring different codes of conduct, or policies towards notice and take down enforcement.¹⁷⁹ Users could host their content on oversea servers, where a freer regime towards speech regulation may apply.¹⁸⁰ If this exit choice is desirable, is something else. Extremist groups, who cannot disseminate their hate speech through German servers, may find a safe

¹⁷⁹ Compare Marsden & Yung 2004, on the willingness of ISPs to cooperate with notice and take down orders.

¹⁸⁰ Compare Zittrain 2003 II, p. 4. On the jurisdictionally evasive practices of Sealand.

harbour in the United States.¹⁸¹ This export of hosting, however, does not offer an exit to the code regulation applied at the destination ISP level in the Internet chain. If content is regulated at this point users have little choice. Enforcement takes place before content may reach them. Obedience is not an option. The choice is made before the user comes into play.

One of the characteristics of code is that it tends to shift speech control from *ex post* to *ex ante* regulation. Instead of prosecution of speech afterwards, the prosecution is automatized and becomes part of the Internet architecture. Speech control is internalized: punishment afterwards is partly replaced by preventive measures. Filtering techniques are built into the network, possibly upstream before either user or content provider can be aware of them. Obviously there still must be the identification of a violation before this violation is regulated. Speech still has to be published before it will entail a reaction to censor it. Though as soon as a violation is established, the process to counter this violation can have the effect of an *ex ante* measure. The spoken becomes unspoken, since the system filters it before users may become aware of it. A public authority may request from an ISP, under the threat of liability, that it blocks certain IP addresses by default. At the moment of this request the addresses may contain non-protected speech, but if this changes, code regulation results in automatic censorship. This raises questions of *accountability*: who can be spoken upon when content is removed? Who is the authority to complain to? But also, who is the authority setting the rules in the first place? The last being a question of legitimacy of code.

In paragraph 4 we have seen the difficulty of accountability of speech regulation on the Internet. Constitutional speech rights are under the traditional framework of law dominated by the idea of vertical and horizontal relationships. This relationship may tilt from vertical to horizontal. Under the vertical relation the judicial branch checks the power granted to the state by its citizens. Fundamental to many modern democracies is the idea of the *trias politica*, which prescribes a division of powers to prevent state abuse. While the executive and legislative powers may be blurred from system to system, the judicial branch has a clear role in controlling state actions against the freedom of speech. For example, towards the regulation of speech on the Internet the US Supreme court has lived up to its role in declaring the *Communications Decency Act* unconstitutional.¹⁸² This left little bitter taste with digital libertarians of the time, but initially took away a lot of attention from the technical regulation of speech through code by private parties. As professor James Boyle put it: 'Once again, the focus on public, criminal and sanction-backed acts by states exercising their power directly, tends to obscure and thus to undervalue the efficacy of efforts that rely on privatized enforcement and surveillance (...)'¹⁸³

With Boyle's observation we come full circle from the introduction of this essay. However, the private surveillance of speech on the Internet may have taken

¹⁸¹ Compare Schumacher 2004 on the legality of the German government's blocking of foreign (hate speech) sites.

¹⁸² *Reno v. ACLU*, 528 U.S. 844 (1997).

¹⁸³ Boyle 1997, IV. 7th paragraph.

another, additional form. The distinction between public and private enforcement should not obscure the hybrid, which can emerge from both spheres. The traditional legal system may have some difficulty responding to it. This essay, at least, will not provide clear answers. We have seen that while code may be used and act as a regulatory tool, there is a friction with Fuller's criteria for law.

We may ask for a clearer distinction by the state of the boundaries between the public and private spheres when it enforces policies towards speech. We may also expect the state to stimulate the transparency of the use of code, especially when it is the main stimulator of this use. Users should be aware of the use and the consequences of speech regulation through network architecture, and be able to claim the speech rights they traditionally enjoyed. Both the setting of code rules and their enforcement ask for more clarity.¹⁸⁴

To conclude, in his analysis of the Panopticon Michel Foucault, not a legal scholar and little experienced "with the hundred impertinent obstructions with which the folly of human laws too often encumbers its operations"¹⁸⁵, did see an architectonic solution to establish clarity and democratic control:

"The Panoptica can even construct a device that supervises its own mechanisms. From the central tower the director can keep an eye on the staff [...] and he, on his turn, will be easily observed. An inspector, who turns up unexpectedly in the centre of the Panopticon, can judge the functioning of the whole institution with one glance, without anything being able to escape his eye. [...] Actually any panoptic institution [...] can be subjected to these accidental but unceasing inspections - and not only by the appointed controllers, but also by the public. [...] So, there is no danger that the increase of power, which the panoptic machinery establishes, results in tyranny; the disciplinary system is being controlled democratically, since it is accessible at any time for 'the highest college of the world tribunal'."¹⁸⁶

¹⁸⁴ To speak with Bentham himself: "The desideratum of clarity represents one of the most essential ingredients of legality." J. Bentham, *The Limits of Jurisprudence Defined*. ... *Compare* Chapter 3, note 95.

¹⁸⁵ The quote is derived from Adam Smith, *compare* note 47 of this essay.

¹⁸⁶ Foucault 1975, pp. ... In a translation of the author.

References

Ahlert & Marsden & Yung 2004

Chr. Ahlert, Chr. Marsden & C. Yung, "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation", May 2004.

American Civil Liberties Union 1997

American Civil Liberties Union, 'Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet', in: Electronic Privacy Information Center, *Filters & Freedom 2.0, Free Speech Perspectives on Internet Content Control*, Washington DC 2001, pp. 97-116.

Baistrocchi 2002

P.A. Baistrocchi, "Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce", *Santa Clara Computer & High Technology Law Journal*, December 2002.

Balkin 2004

J.M. Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society', __ *N.Y.U. L. Rev.* __ (forthcoming 2004).

Blavin & Cohen 2002

J.H. Blavin & I.G. Cohen, 'Gore, Gibson, and Goldsmith: The Evolution of Internet Metaphors in Law and Commentary', *Harvard Journal of Law and Technology*, Vol. 16, No. 1, p. 265, Fall 2002.

Benkler 1998

Y. Benkler, "Communications Infrastructure Regulation and the Distribution of Control over Content", *Telecommunications Policy*, Vol. 22, No. 3, pp. 183-196, 1998.

Benkler 2000 I

Y. Benkler, "Net Regulation: Taking Stock and Looking Forward", *71 U. Colo. L. Rev.* 331, 2000.

Benkler 2000 II

Y. Benkler, "Internet Regulation: A Case Study in the Problem of Unilateralism", *11 European J. of Int'l L.* 167, 2000.

Benkler 2000 III

Y. Benkler, "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access", *52 Fed. Comm. L.J.* 561, 2000.

Biegel 2001

S. Biegel, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, MIT Press 2001.

Birnhack & Elkin-Koren 2003

Michael D. Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment', *8 Va. J.L. & Tech.*, 2003.

Blumenthal & Clark 2001

M.S. Blumenthal & D.D. Clark, 'Rethinking the design of the Internet: The End-to-End Arguments vs. The Brave New World', *ACM Transactions on Internet Technology* Vol. 1, No. 1, August 2001, pp. 70-109.

Boyle 1997

J. Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors', 66 *Univ. Cin. Law Review* 177 1997. Available at <<http://www.law.duke.edu/boylesite>>.

Dommering 2003

E.J. Dommering, 'Grensoverschrijdende censuur: het EHRM en de oude en nieuwe media', in: *Censures/Censuur*, Brussel: Larcier 2003. Compare <<http://www.ivir.nl/medewerkers/dommering.html>>.

Doyle e.a. 2002

J.C. Doyle e.a., *Robustness and the Internet: Theoretical Foundations*, Rough Draft...

Foucault 1975

M. Foucault, *Surveiller et punir, Naissance de la prison*, Paris: Gallimard 1975.

Frydman & Rorive 2002

B. Frydman & I. Rorive, "Regulating Internet Content Through Intermediaries in Europe and the USA", *Zeitschrift fur Rechtssoziologie* 23, Heft 1, S.41-59, 2002.

Geist 2003

M. Geist, 'Cyberlaw 2.0', *Boston college Law Review*, Vol. 44, No. 2, 2003.

Graham 1998

I. Graham, 'Will PICS Torch Free Speech on the Internet?', in: Electronic Privacy Information Center, *Filters & Freedom 2.0, Free Speech Perspectives on Internet Content Control*, Washington DC 2001, pp. 117-124.

Hart 1982

H.L.A. Hart, *Essays on Bentham, Studies in Jurisprudence and Political Theory*, Oxford: Clarendon Press 1982.

Hartman 1998

T.G. Hartmann, 'The Marketplace vs. The Ideas: The First Amendment Challenges to Internet Commerce', *ITSC "Beyond Convergence"*, Stockholm, Sweden, June 21-24 1998.

Heins 2001

M. Heins, 'Filtering Fever', in: Electronic Privacy Information Center, *Filters & Freedom 2.0, Free Speech Perspectives on Internet Content Control*, Washington DC 2001, pp. 1-32.

Hughes 2003

J. Hughes, 'The Internet and the Persistence of Law', *Boston College Law Review*, Vol. 44, No. 2, 2003.

Kerr e.a. 2000

D. Kerr e.a., *Self-labeling and Filtering*, INCORE final report, april 2000. Available at <www.saferinternet.org/downloads/full.pdf>.

Kranich 2004

N. Kranich, *The Information Commons: A Public Policy Report*, New York: Brennan Center For Justice 2004

Lemley 1998

M. A. Lemley, 'The Law and Economics of Cyberspace', *73 Chi.-Kent L. Rev.*1257, 1998.

Lessig & Resnick 1998

L. Lessig & P. Resnick, 'Zoning Speech on the Internet: A Legal and Technical Model', *Michigan Law Review*, vol. 98(2), pp. 395-431. Available at <http://www.si.umich.edu/~presnick/papers/lessig98/>.

Lessig 1999

L. Lessig, *Code and Other Laws of Cyberspace*, New York: Basic Books 1999.

Lessig 2001

L. Lessig, *The Future of Ideas: the Fate of the Commons in a Connected World*, New York: Random House 2001.

Machill & Waltermann 2000

M. Machill & J. Waltermann (red.), *Protecting Our Children on the Internet, Towards a New Culture of Responsibility*, Gütersloh: Bertelsmann Foundation Publishers 2000.

Mailland 2001

J. Mailland, 'Freedom of Speech, the Internet, and the Cost of Control: the French Example', *New York University Journal of International Law and Politics*, Vol. 33, No. 4 2001, pp. 1179-1234. Available at <http://www.nyu.edu/pubs/jilp/>.

McChesney 1999

R. W. McChesney, *Rich Media, Poor Democracy: Communication Politics in Dubious Times*, The New Press: New York 1999.

Moglen 1997

E. Moglen, "The Invisible Barbecue", *97 Columbia Law Review* 945, 1997.

Muller 1993

J.Z. Muller, *Adam Smith in His Time and Ours: Designing the Decent Society*, New York: The Free Press 1993.

Noorlander 2003

P. Noorlander, 'Freedom of Expression and Internet Regulation', in: C. Hardy & C. Möller (ed), *Spreading the Word on the Internet, 16 Answers to 4 Questions*, Vienna: Organization for Security and Cooperation in Europe (OSCE) 2003, pp. 105-115.

Odlyzko 2000

Andrew Odlyzko, 'The history of communications and its implications for the Internet', *AT&T Labs - Research* 2000.

Paul 2000

C. Paul, *Rapport au Premier ministre: Du droit et des libertés sur l'internet; la corégulation, contribution française pour une régulation mondiale*, May 2000. Available at

<<http://www.internet.gouv.fr/francais/textesref/pagsi2/lis/rapportcpaul/sommaire.htm>>.

Radin & Wagner 1999

M.J. Radin & R.P. Wagner, 'The Myth of Private Ordering, Rediscovering Legal Realism in Cyberspace', *Chicago-Kent Law Review* 1999.

Reidenberg 1998

J.R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology', *Texas Law Review*, Vol. 76, No. 3, February 1998.

Reidenberg 2002

J.R. Reidenberg, 'Yahoo and Democracy on the Internet', *42 Jurimetrics J.* 261-280, 2002.

Reidenberg 2004

J.R. Reidenberg, 'States and Internet Enforcement', *1 Univ. Ottawa L. & Tech. J.*, 2004.

Saltzer, Reed & Clark 1984

J.H. Saltzer, D.P. Reed & D.D. Clark, 'End-to-End Arguments in System Design', *ACM Transactions in Computer Systems* 2, 4 November 1984.

Schiff Berman 2000

P. Schiff Berman, 'Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation', *Colorado Law Review*, 2000.

Shapiro 1999

A. L. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, New York: Public Affairs 1999.

Smolla 1992

R.A. Smolla, *Free Speech in an Open Society*, New York: Random House Inc. 1992.

De Sola Pool 1983

I. de Sola Pool, *Technologies of Freedom*, Cambridge: Harvard University Press 1983.

Sunstein 2001

C. Sunstein, *Republic.com*, Princeton: Princeton University Press 2001.

Solum & Chung 2003

L. B. Solum and M. Chung, *The Layers Principle: Internet Architecture and the Law*, University of San Diego School of Law, Public Law and Legal Theory Research Paper 55, June 2003.

Willinger 2002

W. Willinger and J. Doyle, *Robustness and the Internet: Design and evolution*. Available at <http://netlab.caltech.edu/pub/papers/part1_vers4.pdf>.

Wu 1999

T. Wu, 'Application-Centered Internet Analysis', *85 Virginia L. Rev.* 1165, 1999.

Zittrain 2003 I

J. Zittrain, 'Internet Points of Control', *Boston College Law Review*, Vol. 43:1, 2003.

Zittrain 2003 II

J. Zittrain, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law', in: A. Thierer and W. Crews (ed.), *Who Rules the Net?*, Cato Institute 2003.

Zittrain & Edelman 2003

J. Zittrain and B. Edelman, 'Internet Filtering in China', *IEEE Internet Computing*, March/April 2003.

Discussion Points Code as Code Workshop

1. Does utilitarian or security thinking currently overshadow freedom thinking? Do we see a decline of speech rights on the Internet? Is this a trend?
2. Will connectivity be chosen over content on the Internet (see paragraph 2.1.3)?
3. Can geolocation and other techniques reestablish national boundaries and jurisdiction on the Internet (see paragraph 3.3.1.1)?
4. In retrospect, was the fear of PICS based filtering exaggerated (see paragraph 3.3.1.2)?
5. Do governments create a legal environment in which private parties (ISPs) are more inclined to cooperate with law enforcement and perform policing functions?
6. Is the classical concept of sovereignty and the related vertical protection of freedom of speech still desirable in this age?
7. Should the horizontalization of speech rights be (re)considered (see paragraph 4.1)?
8. Will the democratic control by 'the highest college of the world tribunal', as envisioned by Foucault, be realized on the Internet (see paragraph 5.)?
9. What kind of action do you suggest to secure online speech rights, if necessary? Do we need to put more emphasis on the protection of speech rights through technological design?
10. Are there any additional topics that should be described?