State-based internet censorship: attempts or delegated practices and their effects on the free flow and future of the internet.

By Pavlidou Kyriaki, LLM Student, Aristotle University of Thessaloniki

Abstract

Internet featuring a great deal of information dissemination and interactive usage, with an estimated 2 billion number of active users around the world, still manages to keep its "magic", while creating an unparalleled sense of freedom and power of unobstructed expression to its users and non users. For how long though? It is the question imperatively raised. An increasing number of democratic and undemocratic states worldwide have already taken steps or have been considering blocking Internet access, regulating content, or imposing digital filters. However, censorship in the net points out thorny topics like freedom of expression, international enforcement with direct and indirect control of the infrastructure of the web as well as less evident issues like perception of the public, i.e. how transparent is for individuals to understand and realize that censorship occurs, or how free do they feel to express their opinions or make any kind of action on the internet. This paper briefly, yet critically examines the existing Internet censorship regimes in countries like Germany, and Australia on one hand and China, Iran, Saudi Arabia on the other, while it also takes into account the concrete censor systems already working worldwide, the type of content that is being censored and considers the problems or the effectiveness of those filtering technologies. On a more brave notice, it raises concerns about the motives underlying those censoring initiatives and actions and poses the necessity of a broader and more substantial education, as well as democratic legislations instead of censorship methods in producing and maintaining a democratic polity that is compatible with the principles of freedom of expression. Whether it is called a "Combating Online Infringements and Counterfeits Act" (COICA), the most recent act proposed in the United States (20.09.2010) to "combat online infringement", it is for a fact that an ongoing greed for censorship is spreading over the internet, creating an ambiguous and less appealing Internet future to be. The censorship tendency in contrast to the alluring idea of an anarchic Internet, still strangely protective for the users, makes it inevitable but to ask: Do we have to reassess the matter of censorship all over again?

Keywords: Internet / censorship / filtering technologies / delegated regimes / digital filters flaws / transparency / legitimacy.

Introduction

Internet featuring a great deal of information dissemination and interactive usage, with an estimated 2 billion number of active users around the world, still manages to keep its "magic", while creating an unparalleled sense of freedom and power of unobstructed expression to its users or even non users.

For how long though? Now that we are more than 10 years into the Internet revolution [Palfrey, 2007], this is a question that is imperatively raised.

The Internet and wireless technologies have been heralded as vehicles of free expression and it has generally been thought that no government could control information on the Internet [Maurushat], hence the expression that is used "the Internet interprets censorship as damage, and routes around it". However, this does not appear to be the case, anymore. On the 22nd of last September 2010, Google finally came to acknowledge, what transparency and privacy advocates criticised her for as well as what was being voiced long before among scientific communities, was estimated in various organizations reports or was even suspected by internet users; that Internet is for a fact being blocked, in other words is being censored. With the so called *Transparency Report*, an interactive platform that was launched as a deterrent to censorship [1], Google avouched that Internet traffic to Google sites is blocked and that government requests worldwide are frequently made.

One Internet is no longer there [Bambauer, 2009]. The local nature or view of the Internet has changed, so that "one state's Internet does not look the same as another's" [Seltzer, 2008]. An increasing number of democratic and undemocratic states worldwide have already taken steps or have been considering doing so through different legal or technical controls such as blocking Internet access, regulating content, or imposing digital filters. As a result Internet looks different depending on our vantage point of access and the global flow of information is tempered by the activity of the censors.

For oppressive societies, the strongest form of the argument in support of online censorship is that censorship comprises "a legitimate expression of the sovereign authority of states or more simply [an] unalterable right of a state to ensure its national security" [Palfrey, 2007]. On the other hand, in democratic societies, the basis for Internet filtering or other content control amplify issues of copyright infringement, hate speech, sensitive historical facts, defamation, privacy protection or child protection [Dutton, Dopatka, Hills, Law and Nash, 2010].

Censorship in the net though prompts legitimate and normative concerns the most straightforward of which involve civil liberties [Palfrey, 2007] such as the basic rights of freedom of expression and individual privacy while it points out as well thorny topics in relation to international enforcement through direct or indirect control as well as less evident issues like perception of the public, i.e. how transparent is for individuals to understand and realize that censorship occurs, or how free do they feel to express their opinions or make any kind of action on the internet, Subsequently, although the Internet is generally seen as a "forum of free expression, in reality speech on the Internet is subject to unfettered censorship and discrimination at a variety of chokepoints" [Nunziato, 2009].

Anyone of us could easily confirm that and numerate if asked, more than one cases of online censorship that he/she was encountered with or heard of; for instance we are all most probably familiar with China's censorship online status as well as with another well-known example regarding Turkey, which has banned access to YouTube long ago, particularly since 2007, when YouTube refused to take down videos critical of Mustafa Kemal Atatürk. But censorship doesn't occur only in these forms. We experience censorship in everyday life ourselves. Filtering systems in libraries and schools is widespread used in many countries, as it happens here in Greece as well with the implementation of the "Greek School Network Web Filtering" service (http://www.sch.gr in association with www.safeline.gr). It is not unlikely as well that while

wandering on the Net, we might come across certain feedback suggesting that the website is not available ('file not found') or that access has been inhibited by some technical problem (eg 'connection timeout') [McIntyre and Scott, 2008].
This might be a form of censorship, too. In particular, it is possible that the authorities may use this method of "error pages" in order to block some websites of opposition political groupings, media or human rights organisations, that may have deemed unacceptable by them, "deflecting in this way criticism and allowing themselves to claim that they are not censoring Internet content" [McIntyre and Scott, 2008]. If a more transparent and accurate message, 'access blocked by government order' was given instead of an innocent error page, the former allegation of the authorities could not easily stand [McIntyre and Scott, 2008].
Another common trend in democratic societies is censorship to be presented *fait accompli*. The most recent example that comes to our mind is with European Commission's very recent message addressed towards internet providers, warning them not to block Skype VoiP service, or else the so called "principle of Internet neutrality" would be legally put into force [2]. But when did that happen? – We came to ask all of us who use Skype regularly.
However, on the Internet there is more than meets the eye, because the eye "doesn't meet" that much as it turns out. Filtering techniques have already progressed so extensively, in order that Internet experts claim now the appearance of second and third generation censorship methods; those methods create a legal and normative environment along with technical capabilities while they reduce even more the possibility of blowback or discovery [Deibert and Rohozinski, 2010].
Motives underlying those practices vary when approached from different angles, political, economical, ethical, and technological. Censorship is an economic activity, according to some, which also bears political cost [Crandall, Zinn, Byrd, Barr and East, 2007]; for others "the actual result of censorship ex ante" can't be foreseen and support of censorship is done in anticipation of increase in surplus afterwards [Depken]. We incline towards the viewpoint that filtering systems and practices satisfy specific state or private interests depriving users in this way of their right to handle this medium according to their will and needs.
If so, we end up asking: who is the actual user and who believes to be one? Are we the users just a stalking horse, witnessing- in the most optimistic scenario- the actual changes or ignoring them – in the least one –without having a say in the process? Is it all happening in the name of the users and the common good without taking into account the most vital and multitudinous part of this medium, i.e. the users? And do we have to reassess the matter of censorship all over again?
Those questions among others we try to address as follows. Whether it is called a "Combating Online Infringements and Counterfeits Act" (COICA) – the most recent act proposed in the United States (20.09.2010) to "combat online infringement" – it is for a fact that an ongoing greed for censorship is spreading over the internet in democratic and less democratic societies, reflecting on the flow of information and creating an ambiguous and less appealing Internet future to come.

Defining Internet Censorship

"But when we attach a PC to the Internet, we might as well be wading through open sewers. Currently, many ISPs are allowing Internet traffic to flow through their systems completely unfiltered, which is akin to a water authority pumping out raw sewage to its customers to clean for themselves." (ZDNet, 2004)

When we refer to Internet censorship it is an issue that provokes certain confusion. So does the idea of Internet itself. By analogy with the filtering of drinking water, the need for internet

censorship for the same need for water authorities to clean unfiltered water is a good example of what internet censorship is not needed for.
Internet filtering primarily on a state level is not an action willingly set in motion of those who wish to be filtered, as it is with water. People don't need "clean" Internet as they need "clean" water, and certainly they do no need someone to clean it for them. Filtering on the internet most of the times doesn't serve the common good in a sense commonly accepted, it's not an act of grace that facilitates user's road to Internet alleys. Internet it is not something that is piped into one's home where it is passively consumed [McIntyre and Scott, 2008], but on the contrary it takes time, a minimum at least technical knowledge and effort to have Internet step into your house. While filtering is increasingly normal, it should not be seen therefore as natural [Bambauer, 2009].
Internet filtering and blocking, Internet surveillance, net neutrality or online content restrictions are the most commonly used expressions used to describe the current concept of internet censorship. But are they all and each and every one of them different forms of one and the same concept of internet censorship or are they distinguished from it in notion?
When we want to refer to the phenomenon of Internet censorship there is a tendency noticed of Internet filtering techniques being identified with it, so that we end up using "Internet filtering" as synonymous to "Internet censorship" Respectively, ***Internet filtering*** – in Palfrey's wording – refers to the practice by which states restrict citizens from accessing or publishing certain information on the Internet. But should we separate censorship from surveillance? ***Internet surveillance*** refers to the means by which states record, listen in on, or track down conversations that take place over the Internet [Palfrey, 2007]. Internet filtering yet closely related, is distinguished from internet surveillance; moreover, the manner and extent of censorship operations is easier in contrast to that of surveillance which is rather more elusive [Palfrey, 2007]. As it concerns the principle of ***network neutrality*** this one 'holds that, in general, network providers may not discriminate against content, sites, or applications' [Balkin, 2009]; to picture that concept network neutrality "is about the rules of the road for Internet users, and about the relationship between the owners of those roads and the users. Government is asked to make a decision as to which users have priority and whether road charging should be introduced, ostensibly to build wider and faster roads in future" [Marsden, 2009].
All of these terminologies yet similar to each other still differ in certain points of meaning. From our point of view internet filtering and surveillance imply the technology factor existing and have a more technical dimension, while network neutrality implies mostly the human factor behind the web activities and underlines the importance of a more values-based approach. Moreover, according to another scholar intriguing aspect, filtering is shorthand for technology *that implies a choice on the part of the user*, so it is more preferable to talk in more neutral terms using "blocking" or even "censoware" instead of filtering, which are beyond user control [McIntyre and Scott, 2008].
In this paper we focus on the state-based internet censorship practises; in this attempt we will mostly concentrate on the censorship practises and existing filtering regimes, focusing on filtering terminology. However, it is crucial to take into account all of the above terms and to try searching their inner relation combining them in constituting the meaning of Internet censorship.
Referring to state-based internet censorship, we should separate that from private-initiated censorship. Regarding the latter, cooperation with government on behalf of the state is possible to result, but it can also occur exclusively in favour of private sector's interests; an example given is when institutions enable filtering systems in their institutional computer network in order to prevent the recreational use of workplace computers [3]. Another version regards as well the filtering software activated in personal computers with the approval, consent and knowledge of the user; in this case when the user chooses to filter his own individual computer no internet censorship is implied, expect from those cases of censorship when it is implement by one user at

the expense of other co-users that use the same computer. But that is not considered to be a state-based censorship, thus it is another issue to deal with on another paper.
Internet censorship though is not to be fully comprehended yet. To understand this phenomenon we should refer to the "end to end argument" or principle of "end-to-end neutrality" [Zittrain, 2002], which consist a central design principle of the Internet. According to it, the internet protocols are designed to execute relatively simple packet-forwarding function moving data packets from the sender to the receiver without regard to their content or security. As a result, the "intelligence" of the network is placed in the middle of it rather at the end-points [Palfrey,2007] often referred to as "the edges" of the network, resulting to empower this way the end-users of the network, as of the other functions are supposed to be performed at their networks or computers [Bendrath, Mueller, 2010]. Now in order to understand the relation between the end-to-end principle and internet censorship, lets try to picture the following everyday-life scenery.
Imagine at first a daydreaming postal worker, walking on foot delivering the letters he has to deliver or riding his bicycle, hoping on and off in front of every address he has a mail for. In sequence to that reads Lawrence Lessig's well-turned metaphor:

"Like a daydreaming postal worker, the network simply moves the data and leaves interpretation of the data to the applications at either end. This minimalism in design is intentional. It reflects both a political decision about disabling control and a technological decision about optimal network design."

Now imagine, urges us Bendrath and Mueller to their exact words, "a postal worker who is not daydreaming, *but instead*: Opens up *all* packets and letters; reads the content; checks it against databases of illegal material and when finding a match sends a copy to the police authorities; destroys letters with prohibited or immoral content; sends packages for its own mail-order services to a very fast delivery truck, while the ones from competitors go to a slow, cheap sub-contractor […] Imagine also that the postal worker could do this without delaying or damaging the packets and letters compared to his (former, now fired) daydreaming colleague" [Bendrath, Mueller, 2010].
Thereupon, Internet censorship is like the slipped postal worker, which violates this end-to-end principle of network design, by imposing control in the middle of the network rather than at the user level [Palfrey, 2007]. However, in certain occasions – as it will be argued further down – for instance when it goes for authoritarian filtering regimes, filtering does not get to reach the end-user but instead it gets to find its "end" to the ISP's providers, leaving users initially intact.

Locus and Means of Internet Censorship

In order borders of control to be established within the cyber environment, **state-based censorship is localized** at different network nodes. Four of them are singled out in OpenNet Initiative's conclusions (Internet backbone, ISPs, Institutions, Individual computers), which are pointed out - differencing in term more or less - by scholars as well.
Speaking of countries like **China**, with extensive filtering regimes we talk mostly of filtering and blocking schemes going over the backbone of the Internet, affecting internet access through the entire country and being state-directed and implemented on a national level. This prospect notwithstanding being impossible without private actor's cooperation leads mainly to the use of Internet Service Providers (ISPs). Those proceed to block access to certain sites and may be required to monitor and keep records of all or some users with certain online activity, to regulate content or to impose digital filters.
The mandate of the state might also prompt weblog hosting services to include controls that disallow an individual publisher from including certain words in the title of a blog post [Palfrey,

2007 and Travis, 2011]. In addition, blocking and filtering technologies on an institutional-level within extended networks of organizations, companies, public or private services, schools and private enterprises can also occur at the government's behest.

When it comes to the different **means of internet censorship**, the digital age, as Chalaby aptly puts it, has brought a new way of censorship; that is to say for the first time *technology can be used as a means of censorship*. For the first time the instruments of control can be integrated with the medium [Chalaby, 2000]. When dealing with state-based censorship we suggest that there should be a further twofold separation between the different means of control; according to Palfrey censorship can be carried out through the use of technology or through nontechnical means with online controls being imposed by law [Palfrey, 2007 and 2010].
In our point of view, though technology is either way needed. The first form of online control presupposes and is merely supported by technological means inside the cyberspace environment and within its technical boundaries while in the second one the actual control can only be fully achieved under legal and soft forms of power; however some minimum technological support is still required as a prerequisite in order censorship to be implemented. To put it differently, when it comes to censor the Net, controlling influence on the public initially relies on technology either on the whole *or* partly when it comes to the necessity of the human factor with at least a minimum part of technological interference included.
This kind of advanced information technology *or* legal mechanisms and soft controls is what a growing number of states around the world uses in their attempt to control the global flow of information [Palfrey, 2010]. From a reversed point of view, internet censorship has to do with the direct or indirect enforcement of controlling power by the state; when state authorities crucially depend on the intervening medium of technology to impose their desirable measures, then medium-integrated mode of control is the case. On the other hand, when state regulators have immediate access to internet content, then we mostly refer to legally and technologically combined strategies which can be enacted over the net by state ascendance.
However, even if technology in soft control methods is needed more or less, the precondition for the existence of internet technology is the very same precondition of the existence of the Internet. So we come to ask: if law on the Internet needs technology does it have to go the other way round as well? Does technology need law? The questioning that will eventually rise up is whether or not internet technology will turn up to overrule traditional narratives of legitimacy long or short term; so we ask ourselves again: Will code be the law? We will hold back to that thought, as any further analysis is beyond the scope of this paper. A first answer though has already been given by professor Lawrence Lessig. He argued that "code is law" and with this celebrated claim he dramatically highlighted a future where the potential of software architecture will substitute for law in the control of behaviour [McIntyre and Scott, 2008]
Returning to our starting point rewarding the various methods of internet censorship, our interest is focused on the mainly state-based censorship techniques which are presented vide infra. These are the ones referring mostly to the technical approaches attempted as well as those integrated ones, which combine both legal and technical modalities. In the process, questions arise as it concerns the indiscernible circumscriptions between those two broader categories, as the methods used are often the same and are not clearly situated in one or the other category. The key to difference those two is the use of special code or not in order censorship to be accomplished.
According to the OpenNet Initiative (ONI) [4] the basic approaches in which internet filtering occurs is technical blocking, search results removal, take-down of websites and induced self-censorship.

Medium-integrated means of online control

The most apparent mode of online control is through the use of technology [Palfrey, 2007]. When we refer to the technical approaches in which control of access to information on the Internet can be accomplished, we normally speak of internet filtering which then substantiates through technical blocking or removal of search results, according to the OpenNet Initiative. But even before filtering occurs there is a two-step process involved, which breaks down to the use of *rating* and *filtering* software [Chalaby, 2000]. Filtering though doesn't mean rating, and should be separated from it; rating comes first and is then followed by filtering. In particular, rating consists of classifying web content according to the different categories such as violence, nudity and so forth [Chalaby, 2000] and this assortment is based on filtering software or different rating platforms (such as the former Platform for Internet Content Selection {PICS} or the current Protocol for Web Description Resources (POWDER) in addition to others).

i. Technical blocking

A state wishing to filter its citizens' access to the Internet has several initial options, but three of them are commonly used to block access to Internet sites when direct jurisdiction or control over websites is beyond the reach of their authority. Those techniques are IP filtering, DNS filtering and URL blocking using a proxy or keyword searching, which is used accordingly to access specific domain names, IP addresses or WebPages in order to be blocked.
Respectively, "blocking traffic to and from lists of websites specified by their Internet Protocol address (a numerical identifier such as 128.16.64.1) is characterized as the simplest filtering mechanism" [Brown, 2008]. The state places special code on computers that lie between the individual end-user and the broader network [Palfrey, 2007] so that certain data packets with a destination or source address on this list will be blocked from reaching their destination or will be dropped by the routers within ISP networks [Brown, 2008], or used in order information about the content or the creator of the requested address to be obtained. On the other hand Domain Names filtering or poisoning, refers to manipulating DNS information, which involves falsifying the response that is returned by a DNS server [Dutton, Dopatka, Hills, Law and Nash, 2010]. Finally, keyword blocking is a more advanced technique that a growing number of countries are employing (source, ONI). In other words, URL or keyword blocking occurs when the search engine of a web browser which is connected to certain blocking software blocks searches involving blacklisted term *or* filters content based on the words found in URLs provided by the software's rating system rather than on the potential of a dynamic content analysis.

ii. Removal of search web results

This method is used in order undesirable websites to be omitted from search results; that is to say finding the sites more difficult is preferred to blocking access to the targeted sites (source, ONI)

Legal and technical-integrated means of online control

The manner in which this control is exercised varies. Denial for the users to access or publish certain information or demands towards web hosts to remove certain websites due to inappropriate or illegal content according to the state's criteria each time with the threaten of

subsequent legal action, are some forms of this kind of online control. The most commonly encountered ones though according to the OpenNet Initiative have to do with the inducement of self-censorship in addition to those enforcing the take-down and cease of specific websites (source, ONI).
In order for states to carry out online censorship effectively they sometimes take control *into their own hands* by erecting technological or other barriers within the state's confines to stop the flow of bits from one recipient to another private party [Palfrey, 2007]. Where officials have control of domain names servers, it is likely for DNS poisoning to occur; one way is to deregister a domain name that is hosting restricted content so as to make the website invisible to the browsers of those users seeking to access the site (source, ONI).
However, as Palfrey puts it, it is possible for the state to *turn to private parties* as well to carry out the online control as it is unable to carry out filtering on its own. Those private intermediaries are quite often corporations chartered locally or individual citizens who live in that jurisdiction whose services connect one online service to another [Palfrey, 2007].
Through these private points of control (ISPs, Institutions, PCs), censorship is succeeded as depicted in the different portrayals of social life. In particular, ISPs characterized as the most critically situated point of control on the Net can direct the flow of the Internet in multiple ways; they may be asked to prevent subscribers from linking to particular sites, take down "objectionable" sites hosted to their servers [Demont-Heinrich, 2002] or act like gatekeepers monitoring control on certain portals.
Web-based services on the other hand may be required to hand down to state agencies the email addresses or even email content of their users; online telecommunication services may be forced to wiretap online conversations in voice or in the form of instant messages, but in this case it is more likely to speak of internet surveillance; social networks may be asked to provide all sort of information that is uploaded to their servers by end-users. Non-governmental organizations and religious leaders may be required to register before using the Internet to communicate about the topics that they work on [Palfrey, 2010]. Schools may be obligated to filter their networks, or install filtration software on each individual computer they provide (source, ONI). Owners of cyber-cafes may be called upon to report on the identity of a certain Web surfer who used a given PC during a given time interval [Palfrey, 2007], or may be forced upon state order to even have a certain furniture arrangement in their cafes halls, lets say with all computers in a circle arrangement with the screens pointed at the café owner's desk so that he can easily keep sight of all user's online activity.
By reason of this last remark it can be stated that the above mentioned practices build up a suspicious environment for the user which eventually lead to a form of censorship driven by his own will. This induced censorship of oneself is encouraged little-by little in the scope of national or international legislation, under the threat of legal action and state enforcement, through the promotion of social norms or suggestions for compliance with certain domestic habits and practices, or with the use of informal methods of intimidation or penalization.
The blocking of web pages or the constant feeling of users that they are subject to web content restrictions or should be, may be intended – in Palfrey's well-aimed words – to deliver a message to users that state officials monitor Internet usage, making it clear to citizens that "someone is watching what you do online" [Palfrey, 2010]. This perception that the government is engaged in the surveillance and monitoring of Internet activity, whether accurate or not, provides according to ONI another 'strong incentive to avoid posting material or visiting sites that might draw the attention of authorities'. As a result soft controls and regulative state improvisations on legal grounds point at more and more incidents of self-censorship within the Internet.

Medium intergraded or legal and technical integrated methods are considered to be outdated and left behind in the censorship race, as new means of censoring the Net heave in sight featuring

second- and third-generation techniques. According to the most recent documentations and scholar approaches, national filtering schemes as those of China represent the first generation, while second- and third-generation filtering technologies are more subtle, flexible, and even more offensive in character. In this way, legal enforcement seems to take the upper hand as opposed to scenarios of pure technological dominance; these next-generation techniques "employ the use of legal regulations to supplement or legitimize technical filtering measures, extralegal or covert practices, including offensive methods, and the outsourcing or privatizing of controls to ''third parties,'' to restrict what type of information can be posted, hosted, accessed, or communicated online" [Deibert and Rohozinski, 2010].
Examples of next generation techniques include "the infiltration and exploitation of computer systems by targeted viruses and the employment of distributed denial-of-service (DDoS) attacks, surveillance at key choke points of the Internet's infrastructure, legal takedown notices, stifling terms-of-usage policies, and national information-shaping strategies" [Deibert and Rohozinski, 2010].
In regard to these new generation strategies, one filter that has become commonplace for many countries censorship reflex actions and that might have also caught the attention of citizen, is the so called *"just-in-time" filtering*. This filtering technique relates to the phenomenon of a state blocking particular types of speech or other forms of online action at a sensitive moment, rather than in the same, constant way over time [Palfrey, 2010] [5]. Libya is the most recent example. In the most recent political events that conducted in Libya, the government, while routing all wire line Internet connections into the inland through state-owned telecommunications authority and without using authorized private Internet service providers (ISPs) was loade with a serious advantage over controlling Internet on a state base. Therefore, on March 4, 2011, "the authority flipped the *"kill switch"*, which prevented persons in government-held territory such as Tripoli from receiving messages of support for the revolution from the outside world, and slowed images of the revolution from getting out" [Travis, 2011].

Concrete systems and Effectiveness

"If Internet filtering were stock, one would be well-advised to buy it; on-line censorship is on the march, in democratic states as well as authoritarian ones" [Bambauer, 2009].

An increasing number of states around the world take part in censoring what their citizens can see and do on the Internet. The People's Republic of China was among the first to implement national filtering systems at the backbone of the country's Internet, popularly referred to as the ''Great Firewall of China'' and had thereby heralded a different era for the future of the Internet. It has thus even been accepted as to "to have created the first truly 21st Century censorship regime, a regime that could plausibly be modelled in societies that are otherwise democratic" [Fish, 2009]. However, while the ''Chinese-style'' [Deibert and Rohozinski, 2010] of Internet censorship receives considerable attention and acknowledgement, censorship in a range of democratic and undemocratic states worldwide is largely ignored by the majority [Bambauer, 2009].
China may have been the first to have implemented extensive controls over the information that their citizens could access, but certainly it wasn't the last one as it became a paradigm of Internet censorship ever since for other countries that follow at her wake. Many countries around the world have already taken and continue to take heavy measures on the Web while the number of states implementing those kinds of technologies is growing over time, as this trend has been emerging since at least 2002 [Palfrey, 2010].

Existing filtering regimes around the world are well-documented [Palfrey, 2010], mostly based on the work of OpenNet Initiative as well as of the Freedom House [5] and it's Global Index of Internet Freedom [Dutton, Dopatka, Hills, Law and Nash, 2010] as well as on the activities of other organizations such us Reporters Without Boarders and Internet Watch Foundation (IWF). Only in 2007, ONI recorded *41 countries* constructing defensive perimeters by building firewalls at key Internet choke points in order access to undesirable content to be denied to the users [Deibert and Rohozinski, 2010]. In addition, looking at the Government's Request Section at Google's Transparency Report, we notice that *39 countries* have requested that specific content is removed or that information about users using certain Google's services or products is provided (it is noticeable that Iran as well as Saudi Arabia, while implementing extensive filtering systems, are not listed nevertheless among the countries in the given table). Control varies over different forms of content, with most prominent of all, the one related to blogs, social networks and NGOs. However, besides those, control is not limited to filtering or censorship, but takes an upsetting step towards various threats to freedom on the Internet. The most extensive of those involve the arrests of bloggers and Internet users, which has taken a dramatic toll regarding Internet's latest facts; "in particular the Committee to Protect Journalists found that only in 2008, there were, for the first time, more jailed 'cyber-dissidents', such as bloggers, than traditional media journalists" [Dutton, Dopatka, Hills, Law and Nash, 2010].
The intention to censor the Web is a given among various states; what differs among them, democratical or non-democratical ones, is the content they target, how precisely they block it and in what extent citizens get involved in the choice and decision making[Bambauer, 2009].
We will now proceed in presenting some of the main features (including key facts, content that is being censored and means of censorship) of some authoritarian acclaimed filtering regimes in addition to those existing filtering technologies or attempts in democracies with constitutional guarantees of protection of civil rights.
On the one hand, stand those states which can make use of **direct control** to content restrictions mostly by imposing legal force on intermediaries, while on the other we find regimes of **delegated censorship** that do not operate the Internet infrastructure directly but nonetheless control what may be seen there, by implementing indirect filtering through legal pressure upon those who search or index websites [Seltzer, 2008].

In the first category of direct exertion with state interfering in the backbone of the Internet on a country level, we find among a relative handful of countries [Seltzer, 2008], China, Iran and Saudi Arabia.
The "rise of the Chinese Communist Party (CCP) brought with it the continued ideal of control over the dissemination of works and ideas" [Maurushat] and short after an entire censorship empire started spreading around the Chinese hectares of fictional Internet land. So how does this sophisticated Chinese censorship system works? The Internet censorship system in **China –** with a number of about 110 million users as reported in 2005 [Deva, 2008] –, works through nine Internet Access Providers licensed by the government, which provide international network access to regional Internet Service Providers [Brown, 2008]. Routers on the national backbone network are configured to drop packets carrying data to and from blocked websites [Brown, 2008], block domain name servers, censor domestic web hosting services and force Internet users to apply their real names to posts they make to online bulletin boards and discussion sites; moreover mirroring routers are used to slow or stop a user's Internet connection if they go to sites with undesirable terms [Fish, 2009] and "national gateway routers are also configured to reset connections between web browsers and servers that carry data containing keywords" [Brown, 2008].
China censors [6] a wide range of political and religious dissent and human rights activism through her "Great Firewall" [Seltzer, 2008] in addition to most forms of publications and

massive media that are considered to be a threat to the governing regime [Maurushat], violating this way freedom of expression and other civil rights. Those sweeping restrictions, though, against information access may involve more than freedom of expression. According to the interesting remark of Alana Maurushat, regarding the case of SARS, *China has a longstanding tradition of curtailing news deemed harmful to society and to China's image* in order to reduce of public fear and to lessen economic damage in the region. So based in the above rationale, it negatively strikes to us, that China does not hesitate to take even the price of blocking timely information that may have repercussions for the health and welfare of individuals [Maurushat]. Indeed, there are three specific areas, the argument goes on, "where censorship and a lack of accurate information distributed in a timely manner have had unrefuted consequences in China in recent history: AIDS, SARS and Avian Bird Flu" [Maurushat].
However, in our point of view, health and welfare are not what is being at stake through these practices; these are side effects in a battle against what Fish claims to be the actual "underlying purpose of the Great Firewall"; and that is public discourse [Fish, 2009]. In Fish's accurate words, "the CCP does not desire to make any one piece of information completely inaccessible, as it knows that is impossible and that heavy-handed attempts to restrict the Internet more thoroughly will harm certain sectors of the economy. Instead, the CCP seeks to control the flow of stories and information on the Internet by both promoting self-censorship and using its control over the broadband network to prevent potentially damaging information from bubbling up to the e-public's attention in the way that "viral" stories and videos so often do. In this way the CCP can control public discussion while still allowing its citizens substantial access to the wonders of the Internet" [Fish, 2009].
Iran operates a similar to China extensive filtering system, requiring ISPs to block access to over 10 million websites [Brown, 2008], sometimes by blocking unexceptionally a cluster of permissible content deemed nearby an impermissible network standpoint [Palfrey, 2010]. More recently, Iran has taken further measures by qualitatively reducing the speed of international connections to 128kbps, so that blocking access to high bandwidth video streams could work effectively [Brown, 2008].
Saudi Arabia also implements one of the most far-reaching and longest-running filtering regimes while it routes all Web pages through a government proxy. Internet access to citizens was only introduced after many years and only when the state authorities were comfortable that this could be done in a manner that would not violate "the tenants of the Islamic religion or societal norms" (source, Internet Service Unit). In reason of that, the so called Internet Services Unit was activated under the directions of the government of Saudi Arabia so that it can oversee and implement the filtration of web pages in order to block those pages of "an offensive or harmful nature to the society" (source, Internet Service Unit). At the same time the state raised the argument that a state preserves the "right to protect the morality of it's citizens" [Palfrey, 2007] and impressively justified this argument in support of censorship on the Web – otherwise benignly referred to as "usefulness of filtering" in the Internet Service Unit webpage – as a spiritual command deriving form the holy writings and finding a further confirmation to some sporadic and selectively scientific studies provided [8].

Moving on from those examples of content control systems established in authoritarian regimes or democracies – being such in name only – to other countries around the world, it is declared to be true that content control measures have become more prevalent [Dutton, Dopatka, Hills, Law and Nash, 2010] in many countries with democratic political systems . In this second category of delegated censorship, we suggestively refer to Germany and to Australia's unsuccessful attempt to establish online censorship through legislative mandate.
As it concerns **Germany**, a localized version of multinational search companies, such as Google responds to national requests by changing the content provided, so that if someone being in

Germany types for instance "http://google.com" into his/her web browser, he/she will be redirected to google.de, based on Google's geolocation of the IP address from which the requested search was attempted. Pre-designated access though with forced redirection to localized version is also followed by curtailed search results. It is for the time period January to June 2010 that in Google's Transparency Report Germany has the most voluminous action with a total number of 2199 data and items removal requests resulted from court orders that related to defamation in search results, which stands high relative to other countries, while it was the first first European country along with France to impose restrictions on Nazi and other materials hosted overseas [Brown].. A federal government youth protection agency in Germany, named BPjM , sends also URLs for sites that contain content that violates German youth protection law, like content touting Nazi memorabilia, glorification of violence, extreme "pornographic writings" or incitement, and those search results are being removed from google.de (Google-Deutschland), as both pro-Nazi content or content advocating denial of the Holocaust are illegal under German law (source, Google Transparency Report). As a result, searching from Germany for the photos of the Abu Ghraib prisoners posted to Rotten.com – as we did ourselves – will return a depauperated set of results, due to reported illegal content and followed by the redirection to ChillingEffects.org after the phrase "*Aus Rechtsgründen hat Google 8 Ergebnis(se) von dieser Seite entfernt. Weitere Informationen über diese Rechtsgründe finden Sie unter ChillingEffects.org"*[Seltzer, 2008] [9].

Australia on the other hand, has dragged worldwide attention, when decided to "implement Internet censorship using technological means, to mandate filtering legislatively and retrofit it to a decentralized network architecture" [Bambauer, 2008]. With that decision, Australia opened the way and marked a shift by Western democracies towards legitimating Internet filtering, without taking under consideration the alternatives available to combat undesirable information [Bambauer, 2008]. Australia's Liberal Party ultimately, failed to create an Internet censorship, according to recent reports, demonstrating this way that democracy can win over governmental control, once is consolidated and competitive, "with many viable parties and powerful anti-censorship constituencies" [Fish, 2009].

Inadequateness of Censorship Technologies

Internet filtering and blockage mechanisms to control the Internet lack in precision and accuracy, are crude and ineffective [Brown, 2008], therefore being imperfect in general they are circumventable and can be easily evaded. This happens, as citizens with technical knowledge can generally outsmart filters that a state has set in motion; as a result very rarely does any state manage to achieve complete filtering on any topic [Palfrey, 2010]. Pages removed from search results can be accessed with just a little effort as long as someone knowing a link decides to bypass the searching option and navigate directly to the site's address. Likewise users who want to access blocked sites can do so, by using overseas Web proxies or intermediate machines that retrieve Web pages on behalf of them [Brown, 2008] or peer-to-peer systems or single proxy machines in order to enhance privacy protection or even activate technology that will override governmental restrictions measures. As an alternative they are also able to use their own Virtual Private Networks (VPN) as a built-in escape valve in order to have access to a faster, unfiltered Internet [Fish, 2009]. Finally, it is quite possible for someone to still see the full generic set of results and to have full access to the removed sites as far as he forces a search engine to the generic.com-based pages rather than the localized ones [Seltzer, 2008].

Subsequently, a country that proceeds to filter the Internet "must make an "over-broad" or "under-broad" decision at the outset" [Palfrey, 2010]. That is to say, due to the widely extended cyber environment of seamless flow including billions of web-pages and other media, filtering of

this huge material available on the Internet is made impractical and the least effective most of the times, while identification or targeting of one specific web-page for instance is unattainable.
In reason of the above, the filtering techniques being extremely imprecise and often used as a by-product will either filter too much or too little Internet content or may block access to large amounts of legitimate material. In this case, according to the terms used by ONI, filtering regimes will have to deal with underblocking or overblocking results.
Underblocking refers to the failure of filtering to block content targeted for censorship, while *overblocking* stands for those cases when filtering software filter or block content, that they do not intend to block at the first place; this occurs as Internet content is to diverse to be classified and filtering operates most of the times by key words and are therefore unable to take into account contextual information in the process (source ONI). Because of the fact that Web servers typically host many or sometimes thousands of sites, blocking one of them translates into blocking of all the sites hosted on that server. A good example is given by Palfrey who argues that "states make blocking determinations to cover a range of Web content, commonly grouped around a second-level domain name or the IP address of a Web service (such as http://www.twitter.com or 66.102.15.100), rather than based on the precise URL of a given Web page (such as http://www.twitter.com/username), or a subset of content found on that page (such as a particular image or string of text)" [Palfrey, 2010].As a result, being vague, imprecise or even incapable of any rating reasoning, filtering technologies block incoherently large quantities of information that may be suitable and legal for all users, while even sites which have "no affiliation with the offending material may find themselves blocked if the common but crude approach of IP address filtering is used" [McIntyre and Scott]. It worth's mentioning for example that the American Civil Liberties Union (ACLU) found that the use by someone of the consecutive letters 's', 'e', and 'x' in a row, while wandering on search machines, may block sites which contain words such as 'Mars exploration' [Chalaby, 2000]. [10]
However, except from IP address filtering, overblocking can also occur because of DNS poisoning, as it can block access to non-Web services outside the targeted domain region, while same overblocking results occur in merely keyword filters implemented by government routers, based on the lists of forbidden keywords, such as Cleenfeed in United Kingdom [Brown, 2008].

A Matter of Legitimacy

"Legitimate censorship is open, transparent about what is banned, effective, yet narrowly targeted, and responsive to citizens' preferences" [Bambauer, 2009].

In traditional censorship of lets say books, if a government wishes to prohibit access to certain books, it follows a public legislative process, which involves elected representatives in the making of rules for enforcement by public officials [McIntyre and Scott]. However, the above presented inherent flaws of internet filtering and blocking software risk both to the efficiency and accountability among others equally important concerning the common features of the different technologies that are used. Overblocking and underblocking filtering answers the question of the ***effectuality*** and ***openness*** of those practices in a negative way; i.e. why certain information is being restricted of accessing is commonly not answered by the states. ***Narrowness*** of restricted content fails to succeed either; overinclusiveness with overbroad outcomes of innocent content being blocked or underinclusion on the other hand of underbroad filtering systems which fail to block proscribed material [Bambauer, 2009], are the two sides of the coin.
Similarly most of the times, in addition to the above, what is pointed out is the issue of ***transparency***. When it comes to the filtering mechanisms, it is possible that the affected user will receive an email or notification or will be sent a summary that a webpage is out of reach due to

blocking. However, filtering and blocking is often ***opaque*** [McIntyre and Scott] and lacks a great deal of transparency and disclosure of blocked material, methods and frequency of blocking tactics. Browsers who see pages disappear are likely to see the author's explanation, whereas when sites are blocked at a search-engine level, it is up to the search providers to notify their end-users [Seltzer, 2008].
Most of the times, though search engines hold back on this information and leave searchers unaware that *a site they never saw is gone* [Seltzer, 2008] and that filtering is in operation. Among the major search engines only Google gives indication of search results removals due to legal demands, sending removal requests on to the Chilling Effects Clearinghouse where the searcher can see the content of the pages that is missing as well as the identity of those responsible. Google has advanced our knowledge by giving notice of the removals in its results page and sending removal requests on to the Chilling Effects Clearinghouse, http://www.chillingeffects.org (Seltzer, 2008) – a joint project of the Electronic Frontier Foundation and Harvard, Stanford, Berkeley, University of San Francisco, University of Maine, George Washington School of Law, and Santa Clara University School of Law clinics. On more recent events, Google as mentioned above has also launched Google Transparency Report, giving further access to every user.
Among countries operating extensive filtering regimes **Saudi Arabia**, through the above mentioned Internet Services Unit notifies users when access to certain pages is blocked [Brown, 2008] and accepts "suggestions" to block or unblock those or other specific pages that can be made by filling up the "unblock" or "block request form" provided; this certain form of practice is not however followed by other countries with repressive Net policies, such as **China** or **Iran**.
Last but not least comes the issue of the states taking restrictions measures and implementing filtering regimes based on a legitimate cause and on the participation of citizens in decision-making about these restrictions, such that sensors are accountable [Bambauer, 2009]. ***Accountability*** therefore is reflected in the extent to which filtering is being implemented with the consent of public actors and legal rules. On the other hand, some may argue that technological control through filtering is applied automatically, so there is no much space for human intervention and no scope for argument. We address this allegation just further down; we would like to argue here, however, that even if technology in its ***automatic enforcement*** does not exercise discretion against users, depending on code by nature [McIntyre and Scott, 2008], it still raises issues of accountability on the extent that it is used by the state at the expense of public discourse and in order to oppress public discourse. *When basic human rights are jeopardized, no position in favour of censorship can stand based on the fact that we are all – in technological terms – equally censored*.

Do we have to reassess the matter of censorship all over again?

Sigmund Freud made the following observation in 1933: *"What progress we are making. In the Middle Ages they would have burned me. Now they are content with burning my books"*; so, have we learned nothing since Freud made this observation in 1933, asks Professor Brown eminently [Brown, 2008]. Taking it from there we dare to have though that we may haven't made much of a progress whatsoever; have we only gone from burning books to "burning" e-libraries?
It is not the flames like in the Inquisition that "now suppress information but invisible and anonymous digital codes […] that operate behind the screens, not in public places, and end-users may not even be aware of their presence in software packages", argued Chalaby 11 years before [Chalaby, 2000]. In the Middle Ages, image and its force were used to inculcate values, intimidate, and "deploy before all eyes an invisible force" [Foucault, 1977 in Chalaby, 2000]. "If

digital technologies are allowed to become widespread and sophisticated instruments of censorship, they could constitute an invisible, timeless and faceless way of controlling discursive flows in the digital age", predicted Chalaby [Chalaby, 2000]. Or could they not?

What Chalaby aptly described in 2000, is from our point of view only the one cast of a batch that has too many players, too much profit, too much controversy and too much of a future ahead of it until we end up telling that code is actually the bugaboo. Nowadays, code may be masterfully used by states either by implementing it or by threatening for its enforcement and it may well bear a new symbolism for the Internet era; that we should be intimidated by technology as we were intimidated by the medieval rituals. Image may not be used they way it did, but instead it is rather being intentionally avoided; it cannot drag the attention of all eyes at once that easily; it cannot cause fear on the extent that it used to. Yet the image is still at stake; the image that we don't get to see. Everyone uses the Internet but hardly few of the broadband internet users know exactly what they actually use and what they are deprived from in the process. However, eleven years after Chalaby's remarks, what current documentations and scholar approaches give precedence to, are the new generation censorship technologies based on government forces and reflex reactions to dissents combined with extensive self-censorship inducement over technology itself.

Then why are we left back to talk only about technology? It looks like when we talk about it, what we may fear that will happen in the next five minutes may have happened ten minutes before. What we may picture to come in the next decades, may be happening as we speak. So, it is fruitless to seek liability merely on technology. After all what lies underneath is the human factor, as "every technology is extension of the intuition of the man, of the limits of the man himself" [Corasaniti, 1996 in Cammarano, 2002].

McIntyre and Scott have an interesting argument to add. Compared with control through legal instruments, using the internet, they claim, with the implication that we may freely do whatever it is technically possible to do, with no necessity of moral engagement in our activities we may be robed "of moral agency or *responsibility*". If such consequences, they say, were to follow through into wider patterns of social interaction, the consequences for responsibility, and for social ordering generally, of such low trust mechanisms of control might be troubling" [McIntyre and Scott, 2008].

So what is it there to do? We cannot use Internet technology in an uncritical way nor can we blame it for all the "bad" information that it is there on the Internet. So do we have to reassess the matter of censorship all over again?

We believe that there is no need for deconstructing basic concepts pivoting around the phenomenon of Internet censorship, rather than replacing them in their current social context and present facts. What has to be reassessed according to us is a two-drifted matter. First of all, as ONI experts argue as well, there should be a reformation of filtering attempts, in terms of transparency, accountability, and inclusiveness, which could be both desirable and beneficial. Secondly, though, we believe that there should be a revaluation of public perception of Internet censorship and public reaction towards it; there should be a reassessment in what Seltzer calls "Internet Politics".

In sequence to that, legitimacy of filtering "in any particular context requires close examination by reference to issues of transparency, responsibility and accountability in respect of the devising and administering of controls, the purposes for which such controls are deployed, and the consent (or absence of consent) of those whose behaviour is controlled as a result" [McIntyre and Scott, 2008]. Any filtering regime should embrace those cardinal principles along with the imperative need for inclusiveness. In particular:

Accountability is indispensable as it "creates a feedback system where filtering decisions can be challenged and where actors, such as government agencies, must justify and defend their actions or failures to act" [Bambauer, Palfrey, Zittrain, 2004].

Public accountability depends on transparency; "*knowing what is being filtered, by whom, with what purpose and to what extent"* [Dutton, Dopatka, Hills, Law and Nash, 2010]. **Transparency** "requires defining clearly and narrowly the content that is blocked or prohibited; this informs content providers of what material is not permitted and helps citizens understand the values that filtering seeks to implement" [Bambauer, Palfrey, Zittrain, 2004]. Last, but not least comes **inclusiveness**; according to it citizens should be involved in decision making about filtering appropriate material and certain balance of control between public and private actors should be preserved [Bambauer, Palfrey, Zittrain, 2004].

Repressed people of the medieval years have hardly had any rights consolidated and fewer chances or democratic valves towards the enhancement of free speech and free action so that they could protest drastically or immediately against censorship practises. On the other hand, people nowadays enjoy more civil rights, which are constitutionally protected in democratic countries or advocated worldwide and can be put into force through different public conduits.

Even if principles of transparency and accountability are taken care of, the part of inclusiveness and responsibility that brings mainstream users to the front, still remains. "Together"; that's the word that we tend to forget, even in such a participatory medium as Internet. Paraphrasing Balkin's words, we would say that people lack a vested interest in each other [10].

Apart from censorship practices that turn upon civil rights in general, paternalistic intentions of one state or welfare and protection of the people are listed as further reasons for the support of restrictions. What lies at the heart of these arguments though, argues Hosp, is actually *mistrust*. People, the argument goes on, believe that the others are more influenced by "bad" information than they are [Hosp, 2004]. However this has to do with the lack of political engagement to the proceedings taking place on the Internet.

Entrusting Internet decisions on the dissemination of ideas to a market dominated by a few powerful state regulators, drives away people, who may have otherwise been trying to "engage in political debate with those ideas, to canvass online opinion, or to view and create art" [Seltzer, 2008]. Decisions regarding, for instance, "what speech is allowed – and what speech is censored – should not be committed solely to the dictates of the dominant private entities that control expression on the Internet" [Nunziato, 2009]. In Seltzer's remarkable words, "reasonable opinions may differ on the propriety of Internet content control, […] but the Internet's power for information dissemination should at least illuminate that decision" [Seltzer, 2008]. Political institutions play an eminent role and checks of the political process are crucial for the free flow and future of the Internet. In the long run, when people have more political participation rights, they learn how to use the means of discussion and information is more valuable so that it helps to reduce mistrust and dampens the demand for censorship [Hosp, 2004].

Conclusion

Internet's basic functionality does not include censorship [Brown, 2008]. It can be designed in whatever we want it to be designed [Balkin, 2009]; and it was designed to allow the efficient transmission of information between networks around the world.

Not realizing what this practically means for every each and one of us who uses the Internet, could possibly mean the exclusion of us in the designing process or even worse the ignorance of such a process actually taking place. If this happens, Internet danger's to lose its most vital part consisted of the various different ideas and cultural traits that people from around the world bring into the mix.

Subsequently, rating and filtering systems may affect the cultural diversity of cyberspace [Chalaby, 2000] and can have a drastic impact on mainstream Internet users whose have access to information [Brown, 2008] as well as civil society activists, who make extensive use of the

Internet to carry out their work [Deibert and Villeneuve, 2005]. In addition "the kinds of individual creativity by the personal computer (PC), including self-expression in the form of the creation of user-generated content, might be thwarted by the presence of a censorship and surveillance regime" [Palfrey, 2007].

But how is it possible for someone to know that something has been censored when he doesn't know that it was there in the first place? Seltzer is among the ones to point out the political concerns that blocking and filtering raises; it can be hard for the public to know – she argues – whom to blame or how to protest search removals [Seltzer, 2008].

First and new generation technologies continue to work against public awareness and realization is a fighting answer against the escalated, ongoing voices raised, when knowledge about censorship methods is gained. They are much more aggressive and less more visible and they have a reason; to hush the bruit about online censorship and leave people dimly aware of how the Internet works and differs across national boarders.

However, it is our belief, that every person should take his own personal responsibility in the matter of censorship. We cannot go on for ages claiming that we are unaware of internet censorship. Internet censorship is here. However, "a wealth of information creates a poverty of attention," pointed out Herbert Simon out a generation ago, and the wealth of information on the Internet which multiplies at an exponential rate may lead us to new upsetting levels of inertia, when everything will seem to follow the rule : out of sight, out of mind. Until at least it affects us.

For example when a government blocks a website or deletes a weblog comment it is much less public and people may non notice it unless it directly affects them; [Fish, 2009]. We, the mainstream users may notice if the state blocks an entire website, as Turkey did on YouTube, but even we do, the outrage may be limited as competing services can fill the gap [Fish, 2009]. Another case that may also apply is that of the user in good faith. When we *do* have already gained and consolidated the basic principles of free speech and privacy protection, warded by legislative previsions and judicial decisions, it is possible to believe in good faith – while having in the meantime a relatively vague and obscure idea of how internet works – that digital world actually works just like the real world does; therefore, as long as we are constitutionally protected and safe against censorship in the real world we tend to feel safe on the internet as well. So, we stay put; Anaware. Deceived. Indifferrent.

It is said, the free and open, truly, "world wide" Web is what we are after [Palfrey, 2010]. So, do we want it be a dark place that "cybervigilants" [Cammarano, 2002] patrol day and night, while we play carefree in our house until they nock on our door?

If this is a scenario that we choose, eventually Internet will not be a place that we will like to "live in" as it may "very well lead to the end of the Internet as we know it" [Nunziato, 2009]. Citizens will be cut off from information sources and each other and it is quite possible that "the global network value of the Internet will be reduced significantly" [Brown, 2008].

What's need to be apprehended is that Internet cannot remain an "intellectual playground for ever" [Ebbs, 1994] or a 'Wild West', lawless and unregulated territory [Dutton, Dopatka, Hills, Law and Nash, 2010]. However, what is needed at the moment, is what Seltzer calls, "an Internet we have democratically chosen and created" [Seltzer, 2008].

More active participation of users in the decision-making process concerning the use of online filtering systems is mandatory in our commitment to preserve Internet alive *while* transparency among the other above mentioned mechanisms might enable the public towards that direction.

Human rights activists "strive to achieve a balance between the freedom of expression, including the freedom to send and receive information regardless of frontiers or form of government, and private or societal interests in property, security, health, or morals" [Travis, 2011].

Legislative measures against censorship and collective actions in that direction keep pace with the *necessity of individual education*, in producing and maintaining a democratic polity that is compatible with the principles of freedom of expression, individual privacy, freedom of speech.
It is an imperative need that we are well-educated, well-informed, and conscious about the current facts regarding the Internet; it is important that we cultivate our moral fibres knowing what is happening, being aware and committed to the society's causes. Only if we know, we will be able to overcome the indirect, often- invisible, disappearance of public speech from intermediate points in the Internet which mutes the political debate around this censorship and we will be able to unite our pressure to the pressure of human rights activists, against censorship advocates and non governmental organizations (NGOs).
Living in a time of the crisis may well be a crisis of conscious. The less we realize and get the time and information that will help us realize of what is happening on the Internet, the more we get to have an illusion of meaningless choice over our actions on the Internet and the less we get to build up a strong consciousness that will lead us in objecting against those practices, in avoiding manipulation and misleading techniques and in designing an Internet according to what we the users want. Realizing "that communications technology is exposing us to an unlimited array of words and images, including some we might find thoroughly repulsive, it would be a mistake to let traffic cops start pulling people over on the electronic highway" [Rheingold, 1994]. We should stay to the highway and learn how to be in it.
Citizens "who value free expression should call for national debate on [censorship] practices, calling attention to the governments and laws that are the source of pressure and evaluating the effects against free speech principles" [Seltzer, 2008].
A democratic polity in and outside the Internet barriers is what is needed in order the nature of the Internet to be preserved. As Balkin interestingly puts it

"The digital age makes increasingly clear that the point of the free speech principle is to promote not merely democracy, but something larger: a democratic culture. What is a democratic culture? It is a culture in which ordinary people can participate, both collectively and individually, in the creation and elaboration of cultural meanings that constitute them as individuals. Participation in culture is important to us as human beings because, in an important sense, we are made out of culture; we draw on culture to be the sort of individuals we are. […] A democratic culture is not democratic because people get to vote on what culture should be like. It is democratic because people get to participate in the production of culture through mutual communication and mutual influence. Democratic culture invokes a ***participatory idea of democracy****"* [Balkin, 2009].

It was only in 1996 that John Perry Barlow declared [12], with his now famous words, that "not only did they believe that nation-states had no right to interfere with any matter relating to the Internet, [but] they also fundamentally believed that nation-states, in fact, could not do so even if they wished" as Internet's "nature" resists regulation [Raman, 2007]. Soon after, in 1997 the United States Supreme Court declared in relation to the case Reno v. ACLU that " the Internet in encouraging freedom of expression in a democratic society outweighs any theoretical but unproved benefit of censorship" [Chalaby, 2000]. Fourteen years after, those words are today much more contemporary than ever before. To the notion and sense of these words we should return, regarding Internet censorship in our days.
We end this paper in the words heard in this notorious case (i.e. Reno v. ACLU); a case that meant to consist a long lasting compass for Internet in its passage through the rocky patches of our times:

"*Internet is the most participatory form of mass speech yet developed. Its content should remain as diverse as human thought"*"

Notes

[1] According to Niki Fenwick, a Google spokeswoman, on "Google Reports on Government Requests and Censorship", Claire Cain Miller, The New York Times Bits, September 21,2010, available http://bits.blogs.nytimes.com/2010/09/21/google-reports-on-government-requests-and-censorship/ / accessed 10.04.2011

[2] Leigh Ph., 19 April 2011, EU decides against stricter net neutrality rules Legislation to prevent a 'two-speed' internet, with some content arriving faster than others, has been ruled out, available at http://www.guardian.co.uk/technology/2011/apr/19/eu-internet-neutrality-legislation / accessed 20.04.2011.

[3] But is it the same when companies prohibit the use of social networks for example to their employees during their job? See the recent court decision 32/2011 of Athens First Judicial Court regarding the case, available at http://www.enet.gr/?i=news.el.article&id=268598 /accessed 10.04.2011

[4] ONI is a collaborative partnership that joins researchers at the University of Toronto, the Harvard Law School and the SecDev Group in Ottawa, (formerly, the Advanced Network Research Group at the University of Cambridge and the Oxford Internet Institute), source ONI, available at http://opennet.net /accessed 15.03.2011

[4] "For instance, the Chinese state blocked applications such as Twitter and YouTube at the time of the 20th anniversary of the Tiananmen Square demonstrations in June 2009", Palfrey, 2010, p. 12.

[5] Freedom House is an independent nongovernmental organization, which focuses on uncovering efforts to restrict transmission of news and politically relevant communications, while acknowledging that some restrictions on harmful content may be legitimate. It measures restrictions from both government and non-state actors. The key components of the index are access to technology as well as free flow of information and content, Dutton, Dopatka, Hills, Law and Nash, 2010, p. 35,

[6] In January 2010, there has been a significant change conserning Google's relationship with China. Google "continued to auto-censor results on Google.cn until January of 2010 when the search engine announced that the company, along with at least 20 other large corporations, had faced sophisticated cyber-attacks originating from within China. These attacks lead to the theft of intellectual property for Google and the unauthorized access to the e-mail of dozens of human rights activists. Consequently, Google announced that it would stop censoring its search results on Google.cn and operate an unfiltered search engine, even if this meant closing its offices in China", Dutton, Dopatka, Hills, Law and Nash, 2010, p.p.62-63.

[7] God Almighty directed humanity in the Nobel Qur'an in the words of His prophet Joseph: *"He said: My Lord, prison is more beloved to me than that to which they entice me, and were you not to divert their plot away from me I will be drawn towards them and be of the ignorant. So his Lord answered him and diverted their plot away from him, truly, He is the All-Hearer, the All-Knower"* [the underlining to be within the text] Yusuf(12):33 34, http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm / accessed 31.03.2011.

[8] In 2008, when Wendy Seltzer wrote her paper she reported 23 results removed, during the same search, Seltzer, 2008, p.

[9] Another example is given by Brown, when he argues that in 2003 the the Indian government ordered ISPs to block access to a specific Yahoo! Group, many simply blocked access to the entire domain, cutting access to around 12,000 groups (source Deibert and Villeneuve, 2005).

[10] In Balkin's exact words, as it concerns collateral censorship: "Book publishers have a vested interest in the work of their authors, and newspapers have a vested interest in the work of their journalists. But if *A* is not affiliated with *B*, *A* lacks strong incentives to defend *B*'s speech

and every incentive to prevent lawsuits. As a result, to avoid liability, *A* will tend to censor a lot.", Balkin, 2009, p. 110.

[11] In John Perry Barlow's words: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. / We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions. / You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions. You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different……..We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity…….", Raman, 2007, p.1.

References

1. Balkin J. (2009), The Future of Free Expression in a Digital Age, Pepperdine Law Review, Vol. 36, 101-118. Available at SSRN: http://ssrn.com/abstract=1335055
2. Bambauer D. (2008), Cybersieves, Duke Law Journal, Vol. 59, 2009, Brooklyn Law School, Legal Studies Paper No. 149, 1-60. Available at SSRN: http://ssrn.com/abstract=1143582
3. Bambauer D. (2008), Filtering in Oz: Australia's Foray into Internet Censorship, Brooklyn Law School, Legal Studies Paper No. 125, 1-30. Available at SSRN: http://ssrn.com/abstract=1319466
4. Banisar D. (2010), Linking ICTs, the Right to Privacy, Freedom of Expression and Access to Information, East African Journal of Peace & Human Rights, Vol. 16, No. 1. Available at SSRN: http://ssrn.com/abstract=1716969.
5. Bendrath R. and Mueller M. (2010), The End of the Net as We Know it?, Deep Packet Inspection and Internet Governance. Available at SSRN: http://ssrn.com/abstract=1653259.
6. Brown I. (2010), Beware Self-Regulation, Index on Censorship 2010 39: 98-106, avalaible at http://ioc.sagepub.com/content/39/1/98
7. Brown I. (2007), Internet Filtering - Be Careful What You Ask for. Freedom and Prejudice: Approaches to Media and Culture, Kirca S., Hanson L., eds., 74-91, Istanbul: Bahcesehir University Press (2008). Available at SSRN: http://ssrn.com/abstract=1026597.
8. Cammarano, P. (2002), Internet and the Censorship: Is it Legal (And Necessary) to Censor the Web?, 1-23, Available at SSRN: http://ssrn.com/abstract=346861 or doi:10.2139/ssrn.346861
9. Chalaby J.K., New Media, New Freedoms, New Threats, International Communication Gazette , Vol. 62: 19-29.

10. Christof D.H. (2002), Central Points of control and Surveillance on a “decentralized” Net: Internet service providers, and privacy and freedom of speech online, available at http://www.emeraldinsight.com/1463-6697.htm
11. Condon St., (2009), Google-backed tool detects Net filtering, blocking, available at http://news.cnet.com/8301-13578_3-10152117-38.html#ixzz1K0ulvOgv / accessed 14.03.2011.
12. Deibert R., Palfrey J., Rohozinski R., Zittrain J., eds., (2010), Access Controlled: The Shaping of Power, Rights, and Rule in cyberspace, MIT Press.
13. Deibert R., Palfrey J., Rohozinski R.,and Zittrain J., eds., (2008), Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge: MIT Press
14. Deibert R. and Rohozinski R. (2010), Beyond Denial: Introducing Next Generation Information Access Controls, Chapter 1, 1-11, in Deibert R., Palfrey J., Rohozinski R., Zittrain J., eds., (2010), Access Controlled: The Shaping of Power, Rights, and Rule in cyberspace, MIT Press.
15. Deibert R. (2003), Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace, *Millennium - Journal of International Studies* 2003 32, 501-530, available at http://mil.sagepub.com/content/32/3/501
16. Deibert R. and Rohozinski R. (2010), CyberWars, Index on Censorship , 39, 79-90, avalaible at http://ioc.sagepub.com/content/39/1/79
17. Deibert, R. & Villeneuve, N. (2005). Firewalls and Power: An Overview of Global State Censorship of the Internet. In Klang M. & Murray A. (Eds.), Human Rights in the Digital Age,111-124, London: GlassHouse.
18. Depken C.A., The Demand for Censorship, 1-38. Available at SSRN: http://ssrn.com/abstract=300859 or doi:10.2139/ssrn.300859.
19. Deva , S. (2007) , Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?, George Washington International Law Review, Vol. 39, 255-319, 2007. Available at SSRN: http://ssrn.com/abstract=964478
20. Deva S. (2008), 'Yahoo! For Good' and the Right to Privacy of Internet Users: A Critique, Journal of Internet Law, Vol. 11, No. 9, 3-10.Available at SSRN: http://ssrn.com/abstract=1165483
21. Dutton W.H., Dopatka, A., Hills M., Law G. and Nash V. (2010), Freedom of Connection - Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet, Dutton W.H., Dopaka A., Hills M., Law G. and Nash V., Freedom of Connection – Freedom of Expression, Paris: UNESCO, 2011, 1-105, Available at SSRN: http://ssrn.com/abstract=1654464
22. Ebbs J and Rheingold H, (1994), Censorship on the Information Highway, Information Management & Computer Security, Vol. 2 No. 4, 30-31, MCB University Press Limited, 0968-5227
23. Electronic Frontier Foundation, Sites COICA may take offline and why, available at http://www.eff.org/pages/sites-coica-may-take-offline-and-why / accessed 08.11.2010.
24. Edwards, L. (2009), Pornography, Censorship and the Internet, Law and the Internet, L. Edwards & C. Waelde, eds., Hart Publishing, 2009. Available at SSRN: http://ssrn.com/abstract=1435093
25. Esbin B. S. (2009), Net Neutrality: A Further Take on the Debate, Progress & Freedom Foundation: Progress on Point, Vol. 16, No. 26. Available at SSRN: http://ssrn.com/abstract=1529090.
26. Fish E. (2009), Is Internet Censorship Compatible with Democracy?: Legal Restrictions of Online Speech in South Korea, Asia-Pacific Journal on Human Rights and the Law, Forthcoming, 43-96, Available at SSRN: http://ssrn.com/abstract=1489621

27. Gorman G. (2005), China-bashing in the internet censorship wars, Online Information Review, Vol. 29 No. 5, 453-456, Emerald Group Publishing Limited, available at www.emeraldinsight.com/1468-4527.htm
28. Hills J. (2006), What's New? War, censorship and Global Transmission: From the Telegraph to the Internet, The International Communication Gazette, Sage Publications, London, Thousand Oaks&New Delhi 1748-0485, Vol 68 (3), 195-216.
29. Hosp G. (2004), Express Yourself ! Political Participation Rights and the Demand for Censorship, 1-26. Available at SSRN: http://ssrn.com/abstract=591029 or doi:10.2139/ssrn.591029.
30. Kreimer S.F. (2006), Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link. University of Pennsylvania Law Review, Vol. 155, 1-92, No. 11, U of Penn Law School, Public Law Working Paper No. 06-45. Available at SSRN: http://ssrn.com/abstract=948226
31. Marsden Chr. T., Net (2010), Towards a Co-Regulatory Solution, Bloomsbury Publishing Christopher T. Marsden, Neutrality: Towards a Co-Regulatory Solution, Bloomsbury Publishing, 2010. Available at SSRN: http://ssrn.com/abstract=1533428
32. Marsden, Christopher T., Network Neutrality and Internet Service Provider Liability Regulation: Are the Wise Monkeys of Cyberspace Becoming Stupid? (June 8, 2010). Global Policy, Vol. 2, No. 1. Available at SSRN: http://ssrn.com/abstract=1622324
33. Maurushat A. (2008), Anti-Censorship, Benevolent Payloads and Human Rights, UNSW Law Research Paper No. 2008-60, 1-24. Available at SSRN: http://ssrn.com/abstract=1402425.
34. McIntyre T. J. and Scott, C.D. (2008), Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility. Regulating Technologies, Brownsword, R., Yeung, K, eds., Oxford, Hart Publishing, 1-15, Available at SSRN: http://ssrn.com/abstract=1103030
35. Rebecca MacKinnon (2007), Flatter world and thicker walls? Blogs, censorship and civic discourse in China, Springer Science and Business Media, 31-46.
36. Miller Cl. C., (2010), Google Reports on Government Requests and Censorship, The New York Times Bits, available http://bits.blogs.nytimes.com/2010/09/21/google-reports-on-government-requests-and-censorship/ / accessed 10.04.2011
37. Nunziato D. (2008), Net Neutrality, Free Speech, and Democracy in the Internet Age, GWU Law School Public Law Research Paper No. 440, Stanford University Press, Forthcoming; Available at SSRN: http://ssrn.com/abstract=1266365
38. Nunziato D.C. (2005), The Death of the Public Forum in Cyberspace. Berkley Technology Law Journal, Vol. 20, No. 1115; GWU Law School Public Law & Legal Theory Research Paper No. 326, 1-53. Available at SSRN: http://ssrn.com/abstract=1003415.
39. OpenNet Initiative, (2004), A Starting Point: Legal Implications of Internet Filtering, A publication of the OpenNet Initiative, available at http://www.opennetinitiative.org.
40. Palfrey J. G. (2010), Local Nets on a Global Network: Filtering and the Internet Governance Problem. (Chapter in The Global Flow of Information, Jack Balkin, ed., Forthcoming), Harvard Public Law Working Paper No. 10-41, 1-16. Available at SSRN: http://ssrn.com/abstract=1655006
41. Palfrey J. (2007), Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet, chapter 1.5, 69-78.
42. Palfrey J. (2006-2007), Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet. Global Information Technology Report, World Economic Forum, 69-78. Available at SSRN: http://ssrn.com/abstract=978507
43. Raman Ch., Jit Singh (2008), The Regulation of the Internet With Relation to Speech and Expression by the Indian State., 1-66 Available at SSRN: http://ssrn.com/abstract=1237262

44. Segal D. and Swartz, (2010) 09:40 AM , Stop the Internet Blacklist, Huffington Post, Hoffpost Politics, available at http://www.huffingtonpost.com/david-segal/stop-the-internet-blackli_b_739836.html / accessed 1.12.2010.
45. Seltzer W. (2008), The Politics of Internet Control and Delegated Censorship, American Society of International Law, 1-6. Available at SSRN: http://ssrn.com/abstract=1496056.
46. Seltzer W. (2008), The Politics of Internet Control and Delegated Censorship (April 10, 2008). American Society of International Law, Berkman Center Research Publication No. 2008-3, 1-6, Available at SSRN: http://ssrn.com/abstract=1518951.
47. Semitsu, Junichi P., Burning Cyberbooks in Public Libraries: Internet Filtering Software vs. The First Amendment (April 30, 2010). Stanford Law Review, Vol. 52, No. 509, 2000. Available at SSRN: http://ssrn.com/abstract=1598496
48. Sidak, J.Gr., (2004), An Economic Theory of Censorship, Source: Supreme Court Economic Review, Vol. 11, 81-124, Published by: The University of Chicago Press, available at http://www.jstor.org/stable/3655326
49. Accessed: 17/03/2011 11:15
50. Spang-Hanseen H., Stakemann H. (2001), Filtering and Blocking of Websites Content and Legislation on the Internet - Including the Yahoo Case. Kritisk Juss (Norwegian Law Journal - Critical Law), No. 3-4, 321-328. Available at SSRN: http://ssrn.com/abstract=1092384
51. Spang-Hanseen H., Stakemann H. (2001), The Earthly Chaos in Websites Question of Jurisdiction and Net-Censorship. Kritisk Juss (Norwegian Law Journal - Critical Law), No. 1-2, 63-67. Available at SSRN: http://ssrn.com/abstract=1092383.
52. Travis H. (2011), YouTube from Afghanistan to Zimbabwe: Tyrannize Locally, Censor Globally, Florida International University Legal Studies Research Paper No. 11-10, 1-34. Available at SSRN: http://ssrn.com/abstract=1809952
53. Villeneuve N. (2008), Search Monitor: Toward a Measure of Transparency. Available at SSRN: http://ssrn.com/abstract=1157373.
54. Wimmer K. (2006), Toward a World of Law: Freedom of Expression, Annals of the American Academy of Political and Social Science, Vol. 603, Law, society, and Democracy: comparative Perspectives, Sage Publications, Inc in association with American Academy of Political and Social Science, 202-216.
55. Yunchao W., (2010), The Art of Censorship, Index on Censorship 39: 53-57, available at http://ioc.sagepub.com/content/39/1/53
56. *ZDNet*, "Time to filter out the Internet effluent", 18 August 2004. Available at http://news.zdnet.co.uk/leader/0,1000002982,39163885,00.htm / accessed 15.03.2011
57. Zittrain J. and Palfrey J. (2007), Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet, Chapter 5, 103-122, in Deibert R., Palfrey J., Rohozinski R.,and Zittrain J., eds., (2008), Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge: MIT Press.
58. Zittrain J., 2002, Perspective: Can the Internet survive filtering?, available at http://news.cnet.com/2010-1071-945690.html#ixzz1JuWj1fUT / accessed 12.04.2011.